Vysoká škola báňská – Technická univerzita Ostrava

Fakulta bezpečnostního inženýrství

Katedra požární ochrany a ochrany obyvatelstva

Kritická infrastruktura v ČR a EU

Student: Bc. Jan KRAMNÝ

Vedoucí diplomové práce: doc. Dr. Ing. Michail ŠENOVSKÝ

Studijní obor: Bezpečnostní plánování

Datum zadání diplomové práce: 30. listopadu 2009

Termín odevzdání diplomové práce: 30. dubna 2010

Místopřísežně prohlašuji, že jsem celou diplomovou práci včetně příloh vypracoval samostatně.

V Ostravě dne 26. dubna 2010

Jan Kramný

Anotace

Kramný, J: *Kritická infrastruktura v ČR a EU.* Ostrava, 2010, 73 s. Vedoucí diplomové práce doc. Dr. Ing. Michail Šenovský.

Diplomová práce se zabývá problematikou kritické infrastruktury v mezinárodním hledisku. V práci jsou popsány přístupy ČR, EU jako celku, ale také jednotlivých jejích členů, a samozřejmě i dalších zemí světa.

Autor popisuje jednak historický vývoj dané problematiky, tak také současné snahy zemí vedoucí k vymezení jednotlivých oblastí a prvků. Nedílnou součástí je také popis přístupu jednotlivých zemí ke spolupráci soukromého a státního sektoru v oblasti ochrany kritické infrastruktury.

Klíčová slova

Kritická infrastruktura, Ochrana kritické infrastruktury, Česká republika, Evropská unie, Spolupráce soukromého a státního sektoru, Subjekty kritické infrastruktury, Prvky kritické infrastruktury, Krizové plánování.

Anotation

Kramný, J: *Critical Infrastructure in the Czech republic and in the European Union.* Ostrava, 2010, 73p. Supervisor doc. Dr. Ing. Michail Šenovský.

The diploma thesis deals with critical infrastructure in an international perspective. This thesis describes approaches to CR, the EU as a whole, but also its individual members, and indeed other countries in the world.

The author describes the historical development of the issue, as well as current efforts by the countries leading to the delineation of areas and elements. An integral part is a description of how individual countries to work together private and public sectors in protecting critical infrastructure.

Keywords

Critical Infrastructure, Critical Infrastructure Protection, Czech Republic, European Union, Cooperation between the private and public sectors, Operators of critical infrastructure, critical infrastructure elements, Crisis Planning.

Obsah

Seznam tabulek

Úvod

V posledních 20 letech došlo k výrazné změně ohrožení, která mohou mít dopad na zdraví a životy osob, majetek či životní prostředí. Tyto změny můžeme datovat do doby pádu „železné opony“. V době studené války se většina světových zemí připravovala na ohrožení vyplývající z možného vojenského útoku nepřítele. Veškerá opatření, která byla plánována měla z dnešního pohledu charakter civilního nouzového plánování, tedy zajištění chodu státu a podpory ozbrojených sil za války. Po rozpadu Sovětského svazu došlo i ke snížení pravděpodobnosti vzniku válečného konfliktu, a tím pominula i původní ohrožení.

Tím že pominulo ohrožení válkou, vlády zemí si začaly uvědomovat, že existují i jiná rizika. Především rizika vyplývající z průmyslové činnosti člověka a rizika související s přírodními silami. K těmto dvěma základním oblastem se později přidala i rizika související s terorismem. Jednotlivé země si začaly uvědomovat, která odvětví a činnosti jsou nezbytné pro zachování chodu státu, či jsou zranitelné v souvislosti s výše popsanými riziky. Tyto prvky pak souhrnně začínáme označovat jako životně důležitou, nebo také kritickou infrastrukturou.

Jedním ze základních úkolů vlády vyspělého státu je ochrana života a zdraví občanů, majetku, životního prostředí, a zajištění bezpečnosti. Přičemž tyto úkoly musí být naplňovány i v době vzniku mimořádných událostí či krizových situaci.

Jako kritickou danou část infrastruktury označujeme, neboť její činnost je nutná k zajištění základních úkolů státu, a její vyřazení či zničení by mohlo mít nepříznivý dopad na fungování státu.

Cílem práce je zanalyzovat přístup k problematice kritické infrastruktury v zemích EU a České republice.

Rešerše

K vypracování této práce a splnění stanovených cílu bylo potřeba prostudovat materiály, tykající se kritické infrastruktury, a přístupů jednotlivých zemí světa a EU k dané problematice. Jejich přehled a krátké charakteristiky jsou uvedeny níže.

BRUNNER, E.; SUTER, M.: *INTERNATIONAL CIIP HANDBOOK 2008 / 2009 : AN INVENTORY OF 25 NATIONAL AND 7 INTERNATIONAL CRITICAL INFORMATION INFRASTRUCTURE PROTECTION POLICIES*. Series Editors: Andreas Wenger, Victor Mauer and Myriam Dunn Cavelty. Zurich, 2008. 546 s. [16] Publikace pojednává a přístupu k problematice kritické infrastruktury a její ochraně v různých zemí a částech světa.

GORDON, K.; DION, M.: *PROTECTION OF 'CRITICAL INFRASTRUCTURE' AND THE ROLE OF INVESTMENT POLICIES RELATING TO NATIONAL SECURITY*. Paris : France : OECD, 2008. 11 s. [15] Práce se popisuje definice kritické infrastruktury v několika zemích světa. Část je věnována také základnimuu rámci ochrany kritické infrastruktury.

ŠENOVSKÝ, M.; ADAMEC, V.; VANĚK, M.: *Bezpečnostní plánování*. Ostrava : SPBI Spektrum, 2006. 86 s. ISBN 80-86634-52-4. [17] Publikace je zaměřena na problematiku managementu a plánování v oblasti krizového řízení.

ŠENOVSKÝ, M.; ADAMEC, V.; ŠENOVSKÝ, P.: *Ochrana kritické infrastruktury*. Ostrava : SPBI Spektrum, 2007. 141 s. ISBN 978-80-7385-025-8 [18] Publikace přináší čtenáři dostupné informace z oblasti kritické infrastruktury. Jsou zde prezentovány informace o vývoji a současném stavu v dané oblasti, především se zaměřením na ČR a některé zahraniční země.

ŠENOVSKÝ, M.; ADAMEC, V.: *Základy krizového managementu.* Ostrava : SPBI Spektrum, 2004. 102 s. ISBN 80-86634-44-2. [19] Publikace se zabývá základy krizového řízení, plánování a organizační činností, komunikací a přípravou pracovníku v oblasti záchranných služeb.

1 Základní pojmy

Tato část práce se věnuje vymezení základních pojmů, dotýkajících se dané problematiky, a pojmů, se kterými se dále pracuje.

Kritická infrastruktura

Prostředky, systémy a jejich části nacházející se v členském státě, které jsou zásadní pro zachování nejdůležitějších společenských funkcí, zdraví, bezpečnosti, zabezpečení nebo dobrých hospodářských či sociálních podmínek obyvatel a jejichž narušení nebo zničení by mělo pro členský stát závažný dopad v důsledku selhání těchto funkcí.[1]

Evropská kritická infrastruktura

Kritická infrastruktura nacházející se v členských státech, jejíž narušení nebo zničení by mělo závažný dopad pro nejméně dva členské státy. Závažnost dopadu se posuzuje podle průřezových kritérií. To se vztahuje i na účinky způsobené meziodvětvovými závislostmi na jiných typech infrastruktury.[1]

Subjekt kritické infrastruktury

Vlastník nebo provozovatel objektů kritické infrastruktury.[2]

Objekt kritické infrastruktury

Stavba nebo zařízení zajišťující fungování kritické infrastruktury.[2]

Fyzická ochrana kritické infrastruktury

Soubor bezpečnostních opatření plánovaných a realizovaných k ochraně objektů kritické infrastruktury před nebezpečnými útoky fyzických osob.[2]

Mimořádná událost

Škodlivé působení sil a jevů vyvolaných činností člověka, přírodními vlivy, a také havárie, které ohrožují život, zdraví, majetek nebo životní prostředí a vyžadují provedení záchranných a likvidačních prací.[3]

Krizová situace

Mimořádná událost, při níž je vyhlášen stav nebezpečí nebo nouzový stav nebo stav ohrožení státu (dále jen "krizové stavy").[4]

---

[1] Směrnice rady 2008/114/ES, o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu

[2] Terminologický slovník – krizové řízení a plánování obrany státu. Dostupný z WWW: <www.mvcr.cz>.

[3] Zákon č. 239/2000 Sb., o integrovaném záchranném systému, ve znění pozdějších předpisů

2 Infrastruktura

Jako infrastrukturu označujeme vzájemně propojené prvky, které udržují celou strukturu systému pohromadě. V různých odvětvích lidské činnosti může mít tento pojem různý význam. Například pak mluvíme o tzv. infrastruktuře IT, tzn. prvcích tvořící systémy informačních technologií.

Systémy se kterými se každý z nás občanů denně setkává, pak můžeme označit jako infrastrukturu veřejnou, neboli infrastrukturu sloužící k zabezpečení základních potřeb osob. Je tedy velmi důležité tento typ infrastruktury chránit, neboť její zničení či poškození by mělo nedozírné následky na zdraví, životy a majetek osob, ale také na složky životního prostředí.

Dle stavebního zákona č. 183/2006 Sb. rozumíme veřejnou infrastrukturou, pozemky stavby a zařízení, které lze rozdělit do následujících oblastí:

- dopravní infrastruktura – stavby pozemních komunikací, drah, vodních cest, letišť a s nimi souvisejících zařízení
- technická infrastruktura - vedení a stavby a s nimi provozně související zařízení technického vybavení (například vodovody, vodojemy, kanalizace, čistírny odpadních vod, stavby a zařízení pro nakládání s odpady, trafostanice, energetické vedení, komunikační vedení veřejné komunikační sítě a elektronické komunikační zařízení veřejné komunikační sítě, produktovou),
- občanské vybavení - stavby, zařízení a pozemky sloužící například pro vzdělávání a výchovu, sociální služby a péči o rodiny, zdravotní služby, kulturu, veřejnou správu, ochranu obyvatelstva,
- veřejné prostranství - zřizované nebo užívané ve veřejném zájmu, dle zákona č. 128/2000 Sb., o obecním zřízeni (o obcích), ve znění pozdějších předpisů.

V části 1 této práce, pak definujeme co je to kritická infrastruktura, a lze velmi jednoduše dovodit, že součástí KI jsou také prvky právě veřejné infrastruktury. Samozřejmě, nelze použít zjednodušení, že veřejná infrastruktura je kritickou infrastrukturou, ale některé její části pak do kritické infrastruktury řadíme. To tedy v praxi znamená, že je nutné tyto prvky chránit, proti jejich zničení nebo poškození. Přičemž tato ochrana opatření by měla být realizována již v době stavebního řízení (u staveb nových), případně dle rozhodnutí o zařazení staveb mezi prvky KI.

[4] Zákon č. 240/2000 Sb., o krizovém řízení a změně některých zákonů (krizový zákon), ve znění pozdějších předpisů

3 Kritická infrastruktura ve světě

Kritická infrastruktura je jedním z novějších pojmů ve slovníku krizových manažerů. S tímto pojmem je možné se poprvé setkat na konci 90. let 20. století, kdy z původního spojení „Životní infrastruktura“ vzniká ono spojení, známe jako „ Kritická infrastruktura“.

Kritická infrastruktura je v různých zemích světa definována různě. Většinou však definice kritické infrastruktury hovoří, o takové infrastruktuře, která je nezbytně důležitá k zachování základních funkcí států, a jejíž výpadek by měl nežádoucí a nepříznivé účinky na zdraví a životy obyvatel, majetek nebo životní prostředí. Jedná se tedy o tu část infrastruktury, kterou potřebuje k životu každý člověk. Většinou jde o oblasti energetiky, dopravy, státní správy, zdravotnictví apod.

Dále v této kapitole, popisuji přístup k oblasti Kritické infrastruktury v jednotlivých zemích, částech světa a mezinárodních uskupeních. Jedná se zejména o Spojené státy americké, Evropskou Unii a její země, a samozřejmě o mnohonárodnostní vojenské uskupení NATO.

3.1 Kritická infrastruktura v Austrálii

Definice pojmu kritické infrastruktury, jenž Austrálie akceptuje je následující: *„Materiální vybavenost, dodavatelské řetězce, informační technologie a komunikační sítě, při jejichž zničení, degradovaní, nebo dlouhodobém výpadku, by došlo k významnému dopadu na sociální sféru, ekonomiku, zajištění obrany a národní bezpečnosti Austrálie.“* [5]

Zodpovědnost za oblast KI má Generální prokuratura (AGD - Attorney-General’s Department), která vytvořila společnou informační síť pro všechny prvky KI (TISN - Trusted Information Sharing Network for Critical Infrastructure Protection). Celkem je v Austrálii označeno 9 oblastí, které lze označit jako KI, jedná se o:

- komunikace (telefony, faxy, internet, satelity, elektronická hromadná komunikace),
- energetika (plyn, ropná paliva, rafinerie, produktovody, výroba a přenos elektrické energie),
- bankovnictví a finančnictví,
- zásobování potravinami (výroba, skladování a distribuce),

[5] Australian Goverment, Attorney-General’s Department National Security Website. *Http://www.ag.gov.au* [online]. 2006, Last Modified: Friday, 4 September 2009 [cit. 2009-12-27]. Dostupný z WWW: <http://www.ag.gov.au/www/agd/agd.nsf/Page/Nationalsecurity_CriticalInfrastructureProtection>.

- záchranné služby,
- zdravotnictví (nemocnice, veřejné zdraví, vývoj a výzkum),
- hromadné kulturní a sportovní akce,
- doprava (řízení letového provozu, silniční, námořní, železniční doprava, překladiště),
- další služby (zásobování vodou, odpadní vody, nakládání s odpady).

Více než 90% prvků australské KI je ve vlastnictví soukromých subjektů, a jsou provozovány za účelem zisku jejich vlastníků, zbývající prvky pak patří australské vládě nebo teritoriálním vládám. Je tedy dozajisté jasné, že ochrana kritické infrastruktury není možné bez spolupráce a aktivního zapojení soukromého a státního sektoru. Aby byla spolupráce efektivní a přínosná, byly vytvořeny zásady, které by měly všechny strany projektu akceptovat a přijmout za své.

Jak již bylo výše zmíněno odpovědnost za oblast OKI má Generální prokuratura, která spolupracuje s Národním Protiteroristickým Výborem (NCTC – National Counter-Terrorism Committee), jehož primárním úkolem je ochrana australského území před projevy terorismu. Společně tedy vytvářejí strategii ochrany kritické infrastruktury proti terorismu. Australská vláda zodpovídá za analýzu a určení prvků KI, pomoc soukromému sektoru při snižování rizik (pomocí informačních sítí) a spolupráci jak na národní tak také na mezinárodní úrovni. Grafické znázornění systému ochrany australské kritické infrastruktury je součástí příloh (viz. Příloha 1 Systém ochrany KI v Austrálii).

3.2 Kritická infrastruktura v USA

Základem pro definování kritické infrastruktury byl položen v roce 1998, kdy vešlo v platnost směrnice č. 63, tzv. „Bílá kniha“. Tato směrnice byla vydána formou prezidentského rozhodnutí.

Bílá kniha se zaměřuje především na eliminaci následků při vyřazení KI, důraz je kladen na opatření, jež mají snížit zranitelnost systémů. Za nejzávažnější ohrožení jsou v tomto prezidentském rozhodnutí označeny útoky na informační systémy a datové sítě, tedy tzv. kybernetické útoky.

Jako KI jsou tedy v Bílé knize označeny takové systémy a prvky, jejichž základem jsou právě informační systémy a datové sítě (systémy a prvky postaveny na kybernetickém základě).

Hlavní oblastmi jsou pak bankovnictví, telekomunikace, energetika, doprava, zásobování potravinami aj.

Změna v koncepci a pojetí KI v USA přichází bezprostředně po teroristickém útoku na Světové obchodní centrum (WTC) v New Yorku 11. září 2001. Ještě v témže roce je vydáno „Nařízení vlády na ochranu kritické infrastruktury" (Executive Order on Critical Infrastructure Protection).[6] Toto nařízení má za úkol zabezpečení informačních systému kritické infrastruktury. Především pak zajištění nouzové komunikace a ochrany zařízení, která jsou důležitá pro dané informační systémy (budovy, datové rozvody, apod.). Dále je také vydán zákon 107–56 z 21. 10. 2001 (PUBLIC LAW 107–56-OCT. 26, 2001) [1], ve kterém je krom jiného definována KI jako: *„Systémy a zařízení, ať už fyzické nebo virtuální, životně důležité pro Spojené státy, jejichž vyřazení nebo zničení by mělo vliv na bezpečnost, národní ekonomickou bezpečnost, veřejné zdraví, nebo na jejich kombinaci.*"[7]

V roce 2002 byla v USA poprvé vytvořena „Národní strategie vnitřní bezpečnosti"[8] (National Strategy for Homeland Security) [2], která reaguje na události ze září roku 2001. Až teprve v tomto dokumentu jsou poprvé blíže vyjmenovány prvky KI, které jsou v následných letech a dokumentech dále specifikovány. Vytyčuje tři hlavní cíle vnitřní bezpečnosti USA:

1. Předcházeni teroristickým útokům v USA,
2. Sníženi zranitelnosti USA,
3. Minimalizováni škod a následků po útocích.

Další opatření v oblasti KI pak následuji v roce 2003, kdy vstupuje v platnost „Národní strategie fyzické ochrany kritické infrastruktury a klíčových zařízení" (The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets).[9] [3] Tento dokument hovoří o klíčovém prvku národní bezpečnosti, kterým je ochrana kritické infrastruktury. Ochrana kritické infrastruktury je v tomto dokumentu rozdělena do 11 oblastí, a také určuje pět oblastí pro ochranu klíčových zařízení KI, a to takto:

---

[6] Federation of American Scientist: *Executive Order on Critical Infrastructure Protection* [online]. c2008 [cit. 2009-10-28]. Dostupný z WWW: <http://www.fas.org/irp/offdocs/eo/eo-13231.htm>.

[7] *U.S.* Government Printing Service [online]. [1998] [cit. 2009-10-28]. Dostupný z WWW:<http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ056.107.pdf> .

[8] Department of Homeland Security: *National Strategy for Homeland Security* [online]. [1998], October 6, 2008 [cit. 2009-10-28]. Dostupný z WWW: <http://www.dhs.gov/xabout/history/publication_0005.shtm>.

[9] Department of Homeland Security: *The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets* [online]. [1998], January 23, 2009 [cit. 2009-10-28]. Dostupný z WWW: <http://www.dhs.gov/files/publications/publication_0017.shtm>.

1. Oblasti KI:
    a, Zemědělství a potraviny,
    b, Veřejné zdraví,
    c, Vodní hospodářství,
    d, Pohotovostní služby,
    e, Zbrojařský průmysl,
    f, Telekomunikace,
    g, Energetika,
    h, Doprava,
    i, Bankovnictví a finanční sektor,
    j, Chemický průmysl a nebezpečné látky,
    k, Poštovní služby.
2. Klíčová zařízení:
    a, Národní památky,
    b, Atomové elektrárny,
    c, Přehrady,
    d, Vládní zařízení,
    e, Soukromá zařízení.

Národní strategie fyzické ochrany kritické infrastruktury a klíčových zařízení, požaduje vytváření prostředí a politiky, které by podporovaly aktivní zapojení státní správy, soukromého sektoru i občanů USA, při budování systému ochrany kritické infrastruktury.

3.3 Kritická infrastruktura v Kanadě

Kritická infrastruktura je v Kanadě definována jako: *„Fyzická zařízení a zařízení informačních technologií, sítí, služeb a majetku, jejichž narušení nebo zničení by mělo vážný*

dopad na zdraví, bezpečnost, ochranu, hospodářskou stabilitu Kanaďanů nebo efektivní fungování vlády v Kanadě.“[10]

Oblasti, které jsou v Kanadě zahrnuty mezi KI patří:

- energetika a služby,
- komunikační a informační technologie,
- finance,
- zdravotní péče,
- potraviny,
- voda,
- doprava,
- bezpečnost,
- vláda,
- zpracovatelský průmysl.

Kritické infrastruktuře je v Kanadě, věnována pozornost od roku 2001, a to v důsledku reakce na nová ohrožení, která vyplývají ze stále prohlubující se provázanosti fyzické a informační infrastruktury. Roku 2003 je kanadskou vládou sloučeno několik státních institucí a organizací zajišťujících oblast kritické infrastruktury a havarijní připravenosti. Sloučením těchto organizací bylo vytvořeno oddělení Veřejné bezpečnosti a havarijní připravenosti Kanady (PSEPC - Public Safety and Emergency Preparedness Canada). PSEPC, jenž je nyní nazýván jako Úřad veřejné bezpečnosti Kanady (PSC - Public Safety Canada), byl zřízen za účelem ochrany Kanaďanů před účinky přírodních pohrom, kriminality a terorismu. Mezi hlavní povinnosti patří zajištění koordinované pomoci a rozvíjení programů zaměřených na posílení kanadské kritické infrastruktury.

PSC má vedoucí postavení v oblasti OKI, a proto vydává v roce 2008 Národní strategii a akční plán na ochranu KI (National Strategy and Action Plan).[11] Dokument je rozdělen na dvě části, kdy první z nich popisuje Strategii, a druhá je nazvána jako Akční plán, a popisuje

[10] GORDON, K.; DION, M.: *PROTECTION OF ‘CRITICAL INFRASTRUCTURE’ AND THE ROLE OF INVESTMENT POLICIES RELATING TO NATIONAL SECURITY*. Paris : France : OECD, 2008. 11 s.

[11] Public Safety Canada: *Working Towards a National Strategy and Action Plan for Critical Infrastracture* [online]. Kanada , 2008. 2 sv. (38, 38 s.). Dostupný z WWW: <http://www.publicsafety.gc.ca/prg/em/ci/rscs-eng.aspx>. ISBN 978-0-662-48600-8.

konkrétní kroky v oblasti spolupráce. Cílem tohoto dokumentu je vybudovat bezpečnou a mnohem více odolnou Kanadu. Tento cíl má být dosažen díky úzké spolupráci soukromého a státního sektoru (především v oblastech analýzy rizika, a sdílení informací). Každý z prvků spolupráce přináší nové poznatky a náměty, což vede k posílení Kanady v daných oblastech. Převážná část činnosti státu spočívá v poskytování informací, zajištění zapojení soukromého sektoru v oblasti havarijního a krizového plánování a ve spolupráci s dalšími prvky na priorizaci klíčových aktivit každého z 10 odvětví.

Federální vláda má za úkol vytvořit informační síť, pro každý z 10 sektorů, která by umožnila sdílení informací mezi jednotlivými subjekty a státem. Vláda také vytvořila Národní mezioborové fórum (National Cross-Sector Forum), na jehož činnosti se budou podílet zástupci všech sektorů KI. Takto vytvořené seskupení odborníků by mělo především přispět k určení mezioborových závislostí prvků KI, a také by mělo poskytnout rady a doporučení ministerstvu, jak dále postupovat v oblasti ochrany kritické infrastruktury.

Důležitou součástí OKI je i tzv. řízení rizika. Řízení rizika vychází ze zákona vydaného v roce 2007 s názvem zákon o krizovém řízení (Emergency Management Act), který zavazuje představitelé vlády k identifikaci rizik a přípravě na vznik krizových situací, v gesci jejich působnosti. K těmto účelům slouží tvorba plánů a námětová cvičení. Oblast řízení rizik se skládá ze čtyř částí: 1. Zjištění a posouzení rizika; 2. Plány na ochranu nejzranitelnějších prvků KI; 3. Cvičení k prověření správnosti a úplnosti plánů a ochranných opatření; 4. Řízení rizik.

Je zřejmé, že i v Kanadě, je činnost v oblasti KI směřována ke spolupráci veřejného a soukromého sektoru, přičemž státní sektor sehrává roli odborného garanta a vytváří podmínky pro budování systému ochrany KI.

3.4 Norsko

Komise pro ochranu kritické infrastruktury ve zprávě pro ministerstvo spravedlnosti a policie (Ministry of Justice and the police) z roku 2006, definuje kritickou infrastrukturu takto: *„Kritická infrastruktura jsou ty stavby a systémy, které jsou nezbytné k podpoře základních funkcí a potřeb společnosti, a zajištění pocitu bezpečnosti a ochrany u veřejnosti.“*[12]

[12] Commission for the Protection of Critical Infrastructures: *Protection of critical infrastructures and critical societal functions in Norway*. Norsko : [s.n.], 2006. Dostupný z WWW: <http://www.regjeringen.no/upload/JD/Vedlegg/Norwegian_CIP_Commision_-

Na základě této zprávy Komise určila kritické oblasti, které navíc rozděluje na kritickou infrastrukturu a kritické společenské funkce. Jako kritické společenské funkce jsou označovány takové funkce, které jsou nezbytné pro zajištění základních potřeb společnosti. Samozřejmě i tyto společenské potřeby jsou závislé na různých infrastrukturách a to i kritických.

Kritičnost infrastruktury se posuzuje dle tří kriterií:

- závislost – čím vyšší závislost na jiných strukturách tím vyšší kritičnost,
- alternativy – čím méně alternativ tím vyšší kritičnost,
- těsné spojení – vysoký stupeň vazby na ostatní infrastruktury znamená kritičnost.

Mezi kritickou infrastrukturu v Norsku patří:

- elektrická energie,
- elektronická komunikace,
- vodovody a kanalizace,
- doprava,
- ropa a plyn,
- satelitní infrastruktura.

Ke kritickým společenským funkcím dle rozhodnutí Komise patří:

- bankovnictví a finančnictví,
- zásobování potravou,
- zdravotní a sociální služby,
- policie,
- záchranné a nouzové služby,
- krizový management,
- vláda a parlament,
- soudnictví,

_Report_NOU_2006_No_6_English_summary.pdf.upload/JD/Vedlegg/Norwegian_CIP_Commision_-_Report_NOU_2006_No_6_English_summary.pdf.>. s. 20.

- obrana,
- sledování životního prostředí,
- nakládání s odpady.

Výše zmíněná zpráva také popisuje současný stav zajištění ochrany KI v Norsku, a také analyzuje dopad nedávných událostí (vznik nových hrozeb, změny ve vlastnictví infrastruktury, vládní reorganizace) na OKI. Zpráva obsahuje přehled o situaci v jednotlivých oblastech, a také různá doporučení ke zlepšení současného stavu ochrany kritické infrastruktury. Jedno z hlavních doporučení Komise pak uvádí, že vedoucí roli v této oblasti by mělo přebrat Ministerstvo spravedlnosti a policie.

Zodpovědnost za koordinaci v oblasti kritické infrastruktury má Ministerstvo spravedlnosti a policie, avšak celkovou zodpovědnost má Ministerstvo pro záležitosti vlády a reformy (Ministery of Government Administration and Reforms), které tuto úlohu převzalo od Ministerstva průmyslu a obchodu (Ministery of Trade and Industry). V oblasti vojenské bezpečnosti sehrává klíčovou úlohu Ministerstvo obrany (Ministery of Defense).

3.5 Kritická infrastruktura a NATO [14]

V Severoatlantické alianci, je oblast kritické infrastruktury začleněna pod civilní složku NATO, konkrétně spadá pod Civilní nouzové plánování (Civil Emergency Planning). Součástí CEP je tzv. Výbor pro civilní nouzové plánování (Senior Civil Emergency Planning Committee - SCEPC), toto uskupení je vrcholným orgánem pro oblast ochrany civilního obyvatelstva a využívaní civilních zdrojů pro podporu činnosti jednotek NATO. SCECP předává své zprávy přímo Severoatlantické radě (North Atlantic Council - NAC), jenž je vrcholným orgánem NATO. NAC se schází pravidelně každý týden, a je tvořen stálými zástupci členských zemí NATO. Na výši úrovni se pak může setkat ve složení ministrů obrany, ministrů zahraničních věcí a předsedů vlád, přičemž rozhodnutí mají vždy stejnou váhu.[13]

V roce 2003 byla SCEPCem vydána zpráva, která definuje vzájemné závislosti prvků KI, a dále se také zabývá ohodnocením těchto závislostí z pohledu zabezpečení životně důležitých činnosti při vzniku mimořádné události nebo krizové situace. Jedná se tedy o schopnost státu

[13] NATO: *NATO Handbook* [online]. [2000], 17-Jun-2004 [cit. 2009-10-29]. Dostupný z WWW: <http://www.nato.int/docu/handbook/2001/index.htm#CH7>.

reagovat na tyto události. Zpráva definuje 10 činností, jejichž výpadek by mohl mít dopad na prvky KI, a to:[14]

- centrální schopnost reakce,
- zásobování (doplňování) základních služeb,
- místní schopnost reakce,
- dekontaminace,
- místní očista,
- vakcinace a ošetřování,
- péče o hromadně zraněné,
- hromadná evakuace,
- zjišťování ohrožení a jejich pojmenování,
- informování, varování a vyrozumění veřejnosti.

Součástí SCEPC jsou také podvýbory, které zajišťují plánování v několika nejdůležitějších oblastech (např. ochrana obyvatelstva, zdravotní záležitosti, letecká doprava, aj.). Tyto podvýbory zpracovaly několik studii a zpráv z oblasti ochrany kritické infrastruktury. Výsledkem pak bylo rozhodnutí, že ochrana KI (přístup a implementace) je plně věcí jednotlivých členských zemí. Z tohoto důvodu je zaměřena současná činnost NATO v oblasti KI na mezinárodní spolupráci v oblasti vzdělávání, a také sdílení informací co může způsobit výpadek KI, jak jí chránit, a jak v případě potřeby KI obnovit.

[14] GAVENDOVÁ, H.: *KOMPARACE OCHRANY KRITICKÉ INFRASTRUKTURY V ČESKÉ REPUBLICE A EVROPSKÉ UNII*. [s. l.], 2009. 88 s. Masarykova univerzita Brno. Ekonomicko správní fakulta. Vedoucí diplomové práce Ing. Eduard Bakoš.

4 Kritická infrastruktura v Evropské Unii

Tak jako v USA a ve strukturách NATO, tak i na úrovní Evropské unie, začíná být nutné a potřebné řešit otázku kritické infrastruktury. Prvními zeměmi 27, které se oblastí kritické infrastruktury věnují, byly Velká Britanie a Německo. Tyto země již v roce 1999 vydávají nařízení vedoucí k identifikaci a ochraně prvku KI. Ve Velké Britanii je zřízeno Koordinační centrum bezpečnosti národní kritické infrastruktury (National Infrastructure Security Coordination Centre), dále byly také identifikovány systémy, jejichž narušení nebo ztráta by měli dopad na životy osob, oblast hospodářskou a sociální (= systémy důležité pro chod státu). Ve Spolkové republice Německo je projednán návrh „Informačně technické ohrožení klíčových infrastruktur v Německu“. V roce 2001 pak se pak k těmto zemím přidává Nizozemí, kde je vládou přijet „Akční plán bezpečnosti a boje proti terorismu“, který se zaměřuje především na:

- zjištění míry kritičnosti,
- zapojení soukromého a státního sektoru,
- analýzu přijatých opatření.

Na úrovni Evropské unie se pak o KI začíná hovořit, ve větším měřítku až po událostech z let 2004 a 2005, kdy došlo k teroristickým útokům ve španělském Madridu a britském Londýně.

4.1 Historie vývoje KI v EU

V roce 2004 Komise vydává sdělení (Sdělení Radě a Evropskému parlamentu KOM/2004/0702) [4], ve kterém Komise sumarizuje, jaká opatření jsou již v oblasti ochrany KI přijata, a navrhuje i další opatření, která by vedla k posílení stávajícího stavu zabezpečení. Ve svém sdělení Komise upozorňuje, že každá ze zemí EU je povinna určit která infrastruktura je pro ni kritická a stanovit také odpovědné osoby a organizace. Ve Sdělení je uveden i možný přehled potenciálně kritických infrastruktur, a to včetně faktorů určujících kritičnost.

Tabulka 1 Přehled oblastí a prvků KI [4]

Oblast KI	Prvky KI
Energetická zařízení a sítě	elektrická energie, produkce ropy a plynu, skladová zařízení a rafinérie, přenosové a distribuční systémy
Komunikační a informační technologie	telekomunikace, vysílací systémy, software, hardware a sítě včetně Internetu
Finančnictví	bankovnictví, cenné papíry a investice
Zdravotnictví	nemocnice, zdravotnická zařízení a krevní banky, laboratoře a léčiva, pátrací a záchranné služby, pohotovostní služby
Potravinářství	bezpečnost, výrobní prostředky, velkoobchodní distribuce a potravinářský průmysl
Vodní hospodářství	přehrady, skladování, úprava a sítě
Doprava	letiště, přístavy, intermodální zařízení, železniční sítě a sítě veřejné hromadné dopravy, dopravní řídící systémy
Výroba, skladování a přeprava nebezpečných výrobků	chemické, biologické, radiologické a jaderné materiály
Vláda	kritické služby, zařízení, informační sítě, majetek a klíčová státní místa a památky

Faktory dle nichž se určuje kritičnost, jsou celkem tři, a to:

1. Rozsah (hodnocení dle velikosti území, které by bylo postiženo výpadek prvku KI),
2. Závažnost (stupeň dopadu nebo ztráty může být hodnocen jako žádný, minimální, mírný nebo velký)
   a. veřejný dopad,
   b. hospodářský dopad,
   c. dopad na životní prostředí,
   d. politický dopad,
   e. vzájemné závislosti,
3. Vliv času (kdy by mohla mít ztráta prvku vážný dopad = okamžitě, za 24 – 48 hodin, za týden, jindy).

Tabulka 2 Faktory kritičnosti [4]

Faktor kritičnosti	Hodnotící kriterium	Projevy dopadu
Rozsah	jak velké území výpadek ovlivní	mezinárodní, vnitrostátní, oblastní/teritoriální nebo místní
Závažnost	počet postižených osob	postižení jednotlivců, desítek, stovek, tisíců obyvatel
	hospodářství	změny HDP, změny kvality a dostupnosti zboží
	životní prostředí	ztráta druhů, neobyvatelnost lokality
	politická situace	důvěra ve schopnosti vlády a SS
	vzájemná závislost	ovlivnínění jiných prvků KI
Vlic času	kdy má vyřazení vážný dopad	okamžitě, za 24-48 hodin, týden, jindy

Sdělení Komise (KOM/2004/0702) [4] je jedním ze zásadních dokumentu v oblasti KI, neboť krom výše popsaného, hovoří také o vytvoření Evropského programu na ochranu kritické infrastruktury (European Programme for Critical Infrastructure Protection – EPCIC) a Varovné informační sítě pro kritické infrastruktury (Critical Infrastructure Warning Information Network – CIWIN).

Roku 2005 je pak vydána Evropskou unií tzv. „Zelená kniha o Evropském programu na ochranu kritické infrastruktury“ (KOM/2005/0576).[5] Tento dokument se obrací na evropské odborníky, ale také laickou veřejnost, za účelem získání důležitých informací pro směřování EPCIC. Zelená kniha uvádí především základní principy a společný rámec fungování EPCIC, definují se v ní pojmy evropská KI (EKI) a národní KI (NKI). V Zelené knize, jsou také stanoveny povinnosti a role vlastníku, uživatelů a provozovatelů prvků kritické infrastruktury. Evropský program na ochranu kritické infrastruktury se snaží zajistit, aby v celé Unii byla přiměřená a rovnoměrná úroveň zabezpečení KI, přičemž není nutné, aby byly požadavky na zabezpečení pro všechny prvky stejné (odvozují se od dopadu, jaký by měl výpadek daného prvku).

V následných letech je v EU vydána řada dalších materiálů dotýkajících se právě kritické infrastruktury. Jedná se zejména o Sdělení Komise o Evropském programu na ochranu kritické infrastruktury z roku 2006 (KOM/2006/0786; obsahuje zásady, postupy a cíle pro zavedení EPCIC, přičemž obecným cílem je zlepšení zabezpečení ochrany KI) [6] a o usnesení o návrhu Směrnice Rady o určování a označování evropské kritické infrastruktury a

o posouzení potřeby zvýšit její ochranu z roku 2007 (obsahuje základní definice, kritéria pro určování NKI, prvky podpory ze strany Komise).

Na základě Sdělení Komise (KOM/2006/0786) [6] z roku 2006, mají za národní KI (NKI) zodpovědnost členské země, vlastníci a provozovatelé KI. Všechny země EU by tedy na základě tohoto předpisu měli vytvořit národní programy na ochranu kritické infrastruktury, ve kterých by se mělo vycházet z evropských KI (viz. Tabulka 1 Přehled oblastí a prvků KI [4]) a uplatňovat stejné faktory kritičnosti (viz. Tabulka 2 Faktory kritičnosti). Sdělení Komise se také odvolává na společné principy Evropské unie, jež budou uplatňovány pro provádění EPCIP, jedná se zejména o tyto:

- *Subsidiarita* – zaměření na KI, která je kritická z evropského pohledu, avšak v případě potřeby poskytne Komise podporu členským státům v souvislosti s národními KI.
- *Doplňkovost* – pokud je úsilí při ochraně kritické infrastruktury prokazatelně efektivní, nebude jej komise zdvojovat, EPCIP bude tedy navazovat na existující odvětvová opatření a doplňovat je.
- *Důvěrnost* - jak na úrovni EU, tak na úrovni členských států budou informace o ochraně kritické infrastruktury utajovány.
- *Spolupráce zainteresovaných subjektů* – všechny příslušné zainteresované subjekty se v rámci svých možností zapojí do rozvoje a provádění EPCIP. To bude zahrnovat vlastníky/provozovatele kritických infrastruktur označených jako evropské kritické infrastruktury a také státní či další příslušné orgány.
- *Proporcionalita* – opatření budou navržena pouze tam, kde byla na základě analýzy stávajících nedostatků v oblasti bezpečnosti zjištěna jejich potřebnost, a tato opatření budou úměrná úrovni a druhu daného ohrožení.
- *Odvětvový přístup* – jelikož různá odvětví mají odlišné zkušenosti, odborné znalosti a požadavky týkající se ochrany kritické infrastruktury, bude EPCIP rozvíjen podle odvětví a prováděn podle dohodnutého seznamu odvětví ochrany kritické infrastruktury.

4.2 Současné pojetí KI

Posledním a nejnovějším dokumentem v oblasti kritické infrastruktury je Směrnice Rady 2008/114/ES, o určování a označování evropských kritických infrastruktur a o posouzení

potřeby zvýšit jejich ochranu. [7] Jedná se o konečný text výše popsaných Sdělení Komise (KOM/2004/0702 a KOM/2006/0786).[4,6] Směrnice je oproti původním návrhům částečně pozměna a to především v oblasti evropské kritické infrastruktury, kde z původních devíti odvětví zůstali pouze dvě (nazýváme je jako tzv. odvětvové kriterium):

1. Energetika
    a, elektřina (výroba a přenos),
    b, ropa (těžba, rafinace, zpracování, skladování, distribuce),
    c, zemní plyn (těžba, rafinace, zpracování, skladování, distribuce).
2. Doprava
    a, silniční doprava,
    b, železniční doprava,
    c, letecká,
    d, vnitrozemská lodní,
    e, zámořská a pobřežní lodní, přístavy.

Jak je zřejmé již z názvu, zabývá se tato směrnice pouze **evropskou kritickou infrastrukturou (EKI),** což znamená, že na rozdíl od původních návrhů se již nesetkáváme s pojmem národní kritická infrastruktura (NKI) $\Rightarrow$ každá členská země zodpovídá Komisi pouze za EKI v daných dvou oblastech, a je tedy povinna zabezpečit odpovídající úroveň ochrany. Krom odvětvových kriterií, se v rámci této Směrnice uplatňují i tzv. průřezová kritéria, mezi které patří:

1. kritérium obětí (posuzováno podle možného počtu mrtvých či zraněných),
2. kritérium ekonomického dopadu (posuzováno podle závažnosti hospodářské ztráty nebo zhoršení kvality výrobků či služeb, včetně případných dopadů na životní prostředí),
3. kritérium dopadu na veřejnost (posuzováno podle dopadu na důvěru veřejnosti, fyzické strádání a narušení každodenního života, včetně ztráty nezbytných služeb).

Směrnice především upravuje, jakým způsobem se označují EKI a kdo se účastní rozhovorů o označování (vždy stát který označí EKI a další státy, na něž by mělo dopad vyřazení těchto prvků). Dále se také počítá se zřízením funkce Styčného bezpečnostního úředníka, který plní

funkci prostředníka mezi státními orgány a vlastníky/provozovateli KI, přičemž každý stát je povinen zabezpečit vhodnou formu komunikace mezi oběma stranami. Směrnice taktéž ukládá povinnost předkládat zprávy o stavu EKI ve stanovených limitech (do jednoho roku od označení KI za EKI a poté každé dva roky), a na základě těchto zpráv bude posouzeno, zda je nutné přijmout další opatření k ochraně.

Jak je možné zjistit z předchozího textu, oblasti kritické infrastruktury je v EU věnována velká a dlouholetá pozornost. Mechanizmy, jež jsou nastaveny v EU, jsou poměrně zdlouhavé, a proto uběhlo 5 let od doby, kdy se o KI začalo hovořit do doby, než byl schválen a vydán konkrétní dokument, který by zavazoval členské země vyvíjet iniciativu, vedoucí ke zvýšení bezpečnosti v oblasti KI. Lze konstatovat, že EU, respektive její členské země, připravují seznamy evropských kritických infrastruktur a přijímají do svých právních řádů ustanovení Směrnice Rady 2008/118/ES, přičemž implementace směrnice musí být hotova nejpozději do ledna roku 2011.

4.3 KI ve vybraných zemích EU

Přístup jednotlivých členských zemí je v oblasti KI infrastruktury různý. To je dáno především ustanovením Směrnice Rady 2008/118/ES, kde jsou uvedeny vždy pouze minimální požadavky, respektive jsou určeny jen oblasti, které jsou považovány za EKI. Směrnice také zemím umožňuje označovat i další sektory veřejného života za kritické, avšak již nehovoří konkrétněji, jaké sektory by to měli být. Země při výběru dalších oblastí a odvětví KI, musejí postupovat dle přílohy č.3 Směrnice Rady 2008/118/ES, přičemž významnou roli při výběru sehrávají právě průřezová kriteria, která musejí být dodržena aby daná oblast mohla být označena jako evropská kritická infrastruktura. Toto jsou důvody, proč se oblasti kritické infrastruktury mohou v jednotlivých zemích EU lišit. Konkrétní postup jak dochází k zařazení infrastruktury dle přílohy č. 3 Směrnice je uveden v příloze této práce (viz. Příloha 2 Postup k určení EKI).

Následuje přehled několika členských zemí. U každé země je uveden seznam oblastí a prvků KI, a také orgány zodpovídající za oblast kritické infrastruktury.

4.3.1 Německo

Ve Spolkové republice Německo (dále jen Německo), je kritická infrastruktura definována tímto způsobem: *„KI jsou organizace a zařízení mající pro společnost velký význam, a jejichž*

selhání nebo poškození by způsobilo nedostatek dodávek, významné narušení veřejného pořádku nebo jiné dramatické následky.“[15]

Německo přistupuje ke kritické infrastruktuře a její ochraně, tak, že jak vláda, tak také společnost na KI značně závislá. Úkoly státu, které vyplívají z ústavy, jsou: zajištění veřejného pořádku a bezpečnosti, a také zajištění dostatku základních potřeb pro obyvatelstvo. Z těchto úkolů státu lze snadno odvodit, jaké prvky zřejmě patří mezi kritickou infrastrukturu. Jsou jimi:

- doprava a přeprava,
- energetika,
- nebezpečné materiály,
- telekomunikace a informační technologie,
- bankovnictví a finanční služby,
- zásobování (voda, potraviny, zdravotní péče, nouzové a záchranné služby)
- vládní úřady, státní správa a justice,
- média, výzkumné instituce a kulturní statky.

Za koordinaci v oblasti KI, v Německu, zodpovídá Spolkové ministerstvo vnitra (BMI - Bundesministerium des Innern), které společně s dalšími státními úřady a institucemi, vytváří koncepci ochrany KI. Mezi ty, kteří se podílejí na této iniciativě spadají: Spolkový úřad pro informační bezpečnost (BSI - Bundesamt für Sicherheit in der Informationstechnik), Spolkový úřad pro civilní ochranu a pomoc při pohromách (BKK - Bundesamt für Bevölkerungsschutz und Katastrophenhilfe), Spolkový kriminální úřad (BKA - Bundeskriminalamt) a také Spolková policie (BPOL - Bundespolizei). Pro usnadnění koordinace mezi ministerstvem a dalším subjekty, byla v roce 2002 ustavena Meziresortní pracovní skupina Spolkového ministerstva vnitra (Bundesministers des Innern eine interministerielle Arbeitsgruppe - AG KRITIS).

V roce 2005, byly vydány dva klíčové dokumenty, týkající se kritické infrastruktury. Tyto dokumenty lze považovat za začátek mnohých dalších iniciativ v dané oblasti. Těmito dokumenty jsou:

[15] GORDON, K.; DION, M.: *PROTECTION OF ‘CRITICAL INFRASTRUCTURE’ AND THE ROLE OF INVESTMENT POLICIES RELATING TO NATIONAL SECURITY*. Paris : France : OECD, 2008. 11 s.

- Ochrana kritické infrastruktury – výchozí koncept ochrany,[16]
- Národní plán ochrany informační infrastruktury (přijat formou rozhodnutí Spolkové vlády). [17]

Na první z výše jmenovaných pak v roce 2008 navázal jiný dokument s názvem: Ochrana kritické infrastruktury - Řízení rizik a krizového řízení. Průvodce pro firmy a vládní orgány (Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement. Leitfaden für Unternehmen und Behörden.)[18]

Německo také v roce 1999 započalo s aktivitou, jež je nazvána Iniciative D21. Jedná se o největší projekt mezi veřejným a soukromým sektorem, do kterého je zapojeno více než 200 podniků, sdružení, stran, politických institucí a dalších organizací. Hlavními oblastmi, kterými se toto uskupení zabývá jsou:

- digitální integrace,
- digitální technologie, a
- digitální dokonalost.

V oblasti KI je Německo zapojeno také v oblasti mezinárodní spolupráce. Od roku 2003 spolupracuje Spolkové ministerstvo vnitra s Americkým ministerstvem vnitra (US Department of Homeland Security), a to především v oblasti ochrany informační kritické infrastruktury. Německo se také stalo aktivním členem v oblasti budování EPCIC.

4.3.2 Velká Britanie

Spojené království Velké Británie a Severního Irska definuje kritickou infrastrukturu následovně: „*Národní kritická infrastruktura jsou aktiva, systémy a služby, které podporují ekonomický, politický a společenský život ve Velké Británii, a jejichž význam je takový, že jejich zničení by mohlo způsobit: ztráty na životech velkého rozsahu, významně ovlivnit národní hospodářství, mít další vážné sociální dopady, nebo bezprostředně ohrozit vládu.*“[19]

---

[16] Bundesministerium des Innern: *Schutz Kritischer Infratrukturen – Bassisschutzkonzept* [online]. Dostupný z WWW: <http://www.bbk.bund.de>.

[17] Bundesministerium des Innern: *Nationalen Plan zum Schutz der Informationsinfrastrukturen (NPSI)* [online]. Dostupný z WWW: <http://www.bmi.bund.de>.

[18] Bundesministerium des Innern: *Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement (Leitfaden für Unternehmen und Behörde)* [online]. Dostupný z WWW: <http://www.bmi.bund.de>.

[19] GORDON, K.; DION, M.: *PROTECTION OF 'CRITICAL INFRASTRUCTURE' AND THE ROLE OF INVESTMENT POLICIES RELATING TO NATIONAL SECURITY* [online]. Paris : France : OECD, 2008. 11 s.

Jako oblasti, které jsou důležité pro zachování funkčnosti chodu státu, bylo ve VB označeno devět následujících:

- komunikace (data, pevné komunikační sítě, poštovní služby, sdělovací prostředky, bezdrátové komunikace),
- záchranné služby (přednemocniční zdravotnická péče, hasiči, pobřežní stráž, policie),
- energetika (elektřina, zemní plyn, ropa),
- finanční sektor (majetkový management, finanční služby, trhy, investiční a maloobchodní bankovnictví),
- potraviny (produkce, dovoz, zpracování, distribuce, prodej),
- vláda a státní správa (centrální, regionální a místní samospráva, parlamenty a zákonodárné sbory, justice),
- veřejná bezpečnost (CBRN látky, terorismus, hromadné akce),
- zdravotní služby (zdravotní péče, veřejné zdraví),
- doprava (letecká, železniční, silniční a lodní),
- voda (vodovodní řády, kanalizace).

Britská vláda se snaží chránit národní kritickou infrastrukturu proti dvěma druhům hrozeb: fyzickým útokům a elektronickým útokům vůči počítačům a sítím. Hlavní odpovědnost v oblasti KI je v současné době na ministru vnitra VB. Na zajištění ochrany KI se samozřejmě, v oblastech jejích působnosti, podílejí i další ministerstva, která především přispívají odbornými znalostmi. Pro koordinaci činností bylo proto v roce 2007 zřízeno Centrum pro ochranu Národní Kritické Infrastruktury (Centre for the Protection of the National Infrastructure - CPNI). Toto centrum vzniklo spojením Bezpečnostního Koordinačního Centra Národní Infrastruktury (National Infrastructure Security Co-ordination Centre – NISCC) a Národního Poradenského Bezpečnostního Centra (National Security Advice Centre - NSAC).

CPNI spolupracuje jak s veřejnými institucemi, tak se soukromým sektorem. Část ze své odpovědnosti také předává na příslušné státní orgány, které jsou odpovědné za zabezpečení ochrany KI v resortu jejich působnosti (viz. Tabulka 3 Přehled odpovědnosti orgánů SS).

Tabulka 3 Přehled odpovědnosti orgánů SS [16]

Orgán státní správy	Sektor KI
Úřad vlády	vládní a státní služby
Místní samospráva	záchranné služby
Ministerstvo průmyslu	komunikace, energetika
Ministerstvo životního prostředí, výživy a záležitostí venkova	zásobování potravinami a vodou
Ministerstvo dopravy	doprava
Ministerstvo zdravotnictví	záchranné služby, zdravotnictví
Úřad ochrany potravin	potraviny
Ministerstvo financí Jejího Veličenstva	finanční sektor
Mnisterstvo vnitra	záchranné služby

Oblast spolupráce se soukromým sektorem je zaměřena především na sdílení informací mezi CPNI, státními institucemi a provozovateli KI. Cílem je vytvoření mechanizmu, který umožní každému ze zapojených prvků učit se ze zkušeností, omylů a úspěchu druhých, aniž by to mělo to vliv na ochranu citlivých informací (odhalení konkurenci a mediím).

4.3.3 Nizozemí

Kritická infrastruktura je v Nizozemském království definována jako: *„Produkty, služby a doprovodné procesy, které by v případě poruchy nebo selhání, způsobily vážné sociální poruchy. To by mohlo mít formu obrovských ztrát a vážných hospodářských škod…“*[20]

V Nizozemí se s ochranou KI začalo již ke konci 90. let 20. století, přičemž hlavním směrem byla ochrana informačních infrastruktur, toto bylo způsobeno zatím nevyjasněnou definicí kritické infrastruktury. Změna situace nastala v roce 2002, kdy vláda iniciovala vznik projektu na ochranu kritické infrastruktury Ochrana Nizozemské Kritické Infrastruktury (Bescherming Vitale Infrastuctuur). Tento projekt byl složen ze čtyř kroků: 1. Quick-scan analýza pro určení KI a závislostí mezi jejími prvky; 2. stimulace spolupráce veřejného a soukromého sektoru; 3. analýza hrozeb a zranitelnosti; 4. analýza nedostatku ochranných opatření.

V červenci téhož roku pak byly představeny výsledky analýzy Quick-scan, a bylo uskutečněno 17 workshopů, a to jak ve státním, tak také v soukromém sektoru. Navíc skupina odborníků vyhodnotila potenciální ztráty a škody v „životně“ důležitých oblastech a službách.

[20] Ministerie van BZK: *Http://www.minbzk.nl* [online]. [2004] [cit. 2010-01-02]. Dostupný z WWW: <http://www.minbzk.nl/onderwerpen/veiligheid/nationale-veiligheid/vitale/vitale-sectoren-en>.

Tato odborná skupina určila celkem 6 oblastí: Národní a mezinárodní právo, Veřejná bezpečnost, Ekonomika, Veřejné zdraví, Životní prostředí, a Veřejná správa. Bylo konstatováno, že jediný kdo může rozhodnou co je pro chod státu nepostradatelné je samotný stát. Proto rozhodnutí o prvcích kritické infrastruktury, musela učinit vláda.

V roce 2003 nizozemská vláda ve spolupráci se soukromým sektorem, za použití metody Quick Scan, určila 11 oblastí, s celkovým počtem 31 prvků. Následně byla provedena analýza rizika a došlo tak v dubnu 2004 k rozšíření na 12 oblastí s 33 prvky. Jednotlivé oblasti kritické infrastruktury v Nizozemí jsou:

- dodávky pitné vody,
- energetika (elektřina, zemní plyn, ropa),
- finanční sektor (finanční služby a finanční infrastruktura – soukromá i státní),
- potraviny (zásobování a bezpečnost potravin),
- zdravotnictví (neodkladná zdravotní péče, nemocnice, séra a očkovací látky, nukleární medicína),
- právo (justice a vězeňství),
- veřejný pořádek a bezpečnost (zachování veřejného pořádku, udržování veřejné bezpečnosti),
- povrchové vody (řízení kvality vod, zadržování a správa množství vody),
- telekomunikace (pevné sítě, mobilní sítě, rádiové komunikace a navigace, satelitní komunikační služby, rozhlas, přístup k internetu, poštovní a kurýrní služby),
- veřejné služby (diplomacie, informace pro vládu, armádu a ozbrojené síly, rozhodování státní správy),
- doprava (přístav Rotterdam a Schiphol, hlavní pozemní a vodní komunikace, železniční doprava),
- chemický a jaderný průmysl (přeprava, skladování, výroba a zpracování).

Ze strany Nizozemí následují i další kroky v této oblasti, především je určena odpovědnost za oblast KI, a ta spadá do působnosti Ministerstva vnitra (Ministry of the Interior and Kingdom Relations) a jsou nastoleny další kroky v dané oblasti. Ministerstvo v roce 2005 vydává

zprávu určenou pro Nizozemský parlament, ve které jsou definovány nové trendy a cíle v oblasti zajištění ochrany KI. Jedná se především o posílení bezpečnostních politik v oblasti kritické infrastruktury (vytvoření Rady pro OKI - Strategisch overleg Vitale Infrastructuur, SOVI), analýzu závislostí prvků KI (přeshraniční spolupráce jednotlivých provozovatelů), zvýšení odolnosti KI vůči antropogenním hrozbám (ochrana proti terorismu, hackerům, aktivistům, a nespokojeným zaměstnancům; Národní poradenské centrum kritické infrastruktury, poskytuje platformu pro všechny zúčastněné k výměně informací) a zvýšení povědomí občanů (námětová cvičení na národní a regionální úrovni simulující výpadek prvků KI). Průběžné zprávy pak byly předkládány v létech 2006-2007.

Jelikož je i nadále potřeba vyrovnávat se s nově vznikajícími riziky, byla vládou na roky 2007-2008 vytvořena Národní Bezpečnostní Strategie a Pracovní Program 2007-2008 (National Security Strategy and Work Programme for the years 2007–2008), ve které jsou shrnuty cíle bezpečnostní politiky, analýza nebezpečí a rizik, metody vhodné pro strategické plánování. Tento dokument by měl zajistit prohloubení koordinace vnitrostátní bezpečnosti, a má také sloužit jako rámec zásad pro budoucí dění v oblasti OKI. Strategie hovoří o velkém množství rizik, které mohou způsobit výpadek prvků KI. Národní bezpečnost je ohrožena tehdy, dojde-li k poškození zásadních zájmu států nebo společnosti, případně může-li dojít k destabilizaci společnosti. Mezi životně důležité zájmy pak vláda řadí: Územní bezpečnost (terorismus, válka), Ekonomickou bezpečnost (porušení mezinárodního trhu, výpadek telekomunikací), Ekologickou bezpečnost (naturogenní a antropogenní katastrofy, porušní dodávek vody), Fyzickou bezpečnost (porušení hrází, epidemie), Sociální a politickou stabilitu (napětí mezi etniky). Úkolem strategie je identifikovat potenciální hrozby již v jejich zárodku, a předejít tak vážnějším následkům – propojení informačních toků a křížení zdrojů dat (např. v době veder je větší spotřeba energie než v jiných obdobích = předpovědi počasí, zajištění více energie).

4.3.4 Finsko

Kritická infrastruktura (respektive životně důležitá infrastruktura) a pravidla k její ochraně byla poprvé definována již v roce 1992, a to ve vládních dokumentech. Jedná se o zákon o bezpečnosti dodávek (Security of Supply Act) a vyhlášku Národní nouzové zásobovací agentury (Decree of the National Emergency Supply Agency). Tyto oficiální dokumenty stanovují cíle pro zajištění nepřetržitých dodávek v době mimořádných událostí a krizových situací, a jsou aktualizovány každých 5-6 let. Poslední aktualizace proběhla v roce 2008, i když nedošlo k rozšíření prvků KI, byly prvky detailněji definovány.

V současné době jsou oblasti kritické infrastruktury ve Finsku:[21]

- zásobování energiemi a energetické sítě,
- elektronické informační a komunikační systémy (komunikační sítě, IT systémy, mass media, platební systémy bank a pojišťoven),
- doprava a logistika,
- zásobování vodou,
- finančnictví,
- zásobování potravinami,
- zdravotnictví,
- tisk.

Snaha finské vlády je chránit prvky KI za použití nekritických technologií a organizací, a to i během mimořádných událostí a poruch. Základním aspektem v tomto směru jsou technologie umožňující systému zotavení se.

Jak bylo zmíněno problematikou KI se Finsko věnuje již od začátku 90 let 20. Století, kdy snahy byly zaměřeny především na informační bezpečnost. V roce 2005 vláda vydává strategickou rezoluci pro oblast OKI. Na základě rezoluce je pak v roce 2006 vydána Národní strategie povědomé společnosti pro léta 2007-2015 (National Knowledge Society Strategy for 2007–2015), kde je kladen důraz na občany státu, a jejich důvěru v systémy a jejich ochranu.

Státní úřady, které se podílejí na zajišťování ochrany kritické infrastruktury, a vytvářejí podmínky pro realizaci takovýchto opatření, jsou celkem tři:

- Finský telekomunikační regulační úřad (FICORA - The Finnish Communications Regulatory Authority) – spadá pod ministerstvo dopravy a spojů, zabývá se především oblastí regulace a standardizace v oblastí komunikací.
- Řídící výbor pro bezpečnost dat ve státní správě (VAHTI - Steering Committee for Data Security in State Administration) – skupina odborníků začleněna pod správu ministerstva financí, zajišťující bezpečnost informačních technologií.

[21] National Emergency Supply Agency: *Http://www.nesa.fi/* [online]. 2008 [cit. 2009-12-29]. Dostupný z WWW: <http://www.nesa.fi/security-of-supply/objectives/>.

- Národní nouzová zásobovací agentura (NESA - National Emergency Supply Agency) – je podřízena ministerstvu dopravy a spojů, analyzující rizika a hrozby vzhledem ke KI, dále také vytváří podmínky pro spolupráci státního a soukromého sektoru, a také zajišťuje zásobování v době MU a KS.

4.3.5 Francie

Ve Francii se jako kritická infrastruktura označuje veškerá infrastruktura, která je životně důležitá pro zachován základních sociálních a ekonomických procesů. Mezi odvětví, která patří k francouzské KI patří:

- finanční sektor,
- průmysl,
- energetika,
- soudnictví,
- zdravotnictví,
- výkon státní správy,
- elektronická komunikace a informační technologie,
- doprava,
- zásobování vodou,
- zásobování potravinami,
- vesmír a výzkum,
- ozbrojené síly.

V létě 1997 byla ministerským předsedou ustavena informační a komunikační asociace, která měla za úkol vytvořit vzdělanou společnost v oblastech informačních technologii a internetu. Následně pak byl vytvořen Vládní program pro informační společnost (PAGSI – Government Action Program for an Information Society), jehož hlavní úkol spočíval ve zpřístupnění vládních služeb prostřednictvím internetu.

Roku 2006 byla vydána vyhláška o ochraně základních ekonomických sektorů (Décret n°2006-212 du 23 février 2006 relatif à la sécurité des activités d'importance vitale). Cílem této vyhlášky je aktualizovat předpisy týkající se chyb zabezpečení. Aby byl cíl splněn je potřeba harmonizovat přístup jednotlivých odvětví k analýze rizik.

Každé z 12 hospodářských odvětví, které jsou uvedeny v národní bezpečnostní směrnici, mají za úkol vytvořit vlastní bezpečnostní operační plán. Na zpracování plánů dohlíží jednotlivá ministerstva v rámci své působnosti. Obdobné plány kromě podniků zpracovávají i důležité státní orgány a subjekty. Takto vzniklý plán musí být dále upraven pro jednotlivé kritické body, a státním orgánům pak slouží jako podklad k vypracování plánu vnější ochrany.

Oblastí národní a mezinárodní bezpečnostní politiky se zabývá Generální tajemník pro národní obranu (SGDN - The Secretary general for National Defense). Za úkoly spojené s ochranou KI zodpovídají Ústřední ředitelství bezpečnosti informačních systémů a Ministerská komise pro bezpečnost.

4.3.6 Maďarsko

Maďarsko přistoupilo k programu EU na ochranu kritické infrastruktury (EPCIP) již v roce 2005, ale některé politiky v oblasti OKI byl implementovány již dříve. Definice KI v Maďarsku je shodná s definicí uvedené v Zelené knize, a zní: *„Vzájemně propojené interaktivní a vzájemně závislé prvky infrastruktury, zařízení, služeb a systémů, které jsou životně důležité pro fungování národního hospodářství a veřejných služeb, pro udržení přijatelné úrovně bezpečnosti pro národ, životy občanů, a soukromého majetku, stejně jako pro udržení hospodářství, služeb, veřejného zdraví a životního prostředí.“*[22] Oblasti KI v Maďarsku jsou následující:

- informační a telekomunikační systémy,
- energetika,
- zásobování vodou,
- doprava,
- veřejné zdraví,
- zásobování potravinami,
- bankovnictví a finanční sektor,
- průmysl,

[22] BRUNNER, E.; SUTER, M.: *International CIIP Handbook 2008/2009 – An Inventory of 25 National and 7 International Critical Information Infrastructure Protection Policies.* Zurich [online]. ETH Zurich - Center for Security Studies, 2008, 648 p. Dostupný z WWW: <http://se2.isn.ch/serviceengine/FileContent?serviceID =11&fileid=8EAC1DE9-1B8D-DA5B-93D7-4FC32E2415B2&lng=en>.

- státní správa,
- veřejná bezpečnost a obrana.

Po roce 2006, kdy došlo ke změně organizace na vládní úrovni, způsobené volbami, hlavní iniciativa souvisí s přidělením jednotlivých oblastí KI ministerstvům. Tato situace byla způsobena sloučením několika ministerstev, pod která oblast OKI spadala.

V Maďarsku také funguje spolupráce státního a soukromého sektoru v této oblasti. V roce 1992 byla založená nezisková organizace Theodora Puskáse, jejíž hlavním úkolem bylo rozvíjet informační technologie v zemi.

4.3.7 Slovensko

Slovenská republika definuje kritickou infrastrukturu takto: *„Ta část národní infrastruktury (vybrané organizace, instituce, objekty, soustavy, zařízení, služby a systémy), jejichž zničení nebo vyřazení v důsledku působení rizikového faktoru způsobí ohrožení nebo narušení politického a hospodářského chodu státu nebo ohrožení životů a zdraví obyvatel.“*[23]

V současnosti není problematika KI řešena žádným právně závazným dokumentem, ale i přes tuto skutečnost byla v dokumentu Koncepcia kritickej infrastruktury v Slovenskej republike a spôsob jej ochrany a obrany [8], nadefinována kriteria, podle kterých se KI určuje.

Oblasti KI se určují následovně – pokud vyřazení infrastruktury způsobí narušení některé oblasti bezpečnosti státu, pak se jedná o KI. Mezi oblasti bezpečnosti státu řadíme:

- politický chod státu a státní správy,
- obrana státu,
- státní hospodářství,
- životy, zdraví a majetek obyvatel,
- dopravu, informační a komunikační systémy,
- životní prostředí.

Jednotlivé oblasti KI se dále skládají z prvků, pro jejich určení slouží následující kriteria:

[23] Ministerstvo vnútra Slovenskej republiky: *Koncepcia kritickej infraštruktúry v Slovenskej republike a spôsob jej ochrany a obrany* [online]. Bratislava, 2006. 19 s. [cit. 2010-01-02]. Dostupné z WWW: <http://www.minv.sk/?ochrana-kritickej-infrastruktury>.

- pravděpodobnost – s jakou pravděpodobností se daný prvek může stát terčem teroristického útoku, případně jak může být prvek ohrožen jinými rizikovými faktory,
- neakceptovatelné riziko – pokud prvek způsobí, na základě útoku nebo působení jiného faktoru, ohrožení nebo narušení politického chodu státu či jeho obranyschopnosti,
- jedinečnost prvku – pokud je prvek jediný svého druhu a nelze je žádným způsobem nahradit,
- generalizace – existuje-li skupina prvků se stejnou funkcí, ale nelze přesně odhadnout jaké konkrétní prvky by mohly být vyřazené či zničené,
- exkluzivita (doplňkové kriterium) – pokud není prvek národní infrastruktury prvkem žádné oblasti KI (nelze zařadit podle předchozích kriterií), ale existuje nutnost jej označit za prvek KI.

Oblasti KI které jsou na Slovensku určeny, vycházejí z dokumentu Národný program pre ochranu a obranu kritickej infraštruktúry v Slovenskej republike [9], vydaným v roce 2007. Mezi oblasti KI patří:

- voda,
- potraviny,
- zdravotnictví (nemocnice, ochrana veřejného zdraví, léčiva),
- energetika (elektroenergetika, plynárenství, ropa, těžba a hutnictví),
- informační a komunikační technologie,
- doprava (silniční, železniční, letecká a říční),
- veřejný pořádek a vnitřní bezpečnost (pohotovostní složky – CO, hasičský a záchranný sbor, policie, obranný průmysl)
- průmysl (chemický, farmaceutický)
- finanční sektor (platební systémy, účetní systémy, banky, pojišťovny).

Jelikož není žádný právní předpis v oblasti OKI, který by stanovoval odpovědnost orgánů státní správy, je v současné době ochrana kritické infrastruktury svěřena do gesce Ministerstva vnitra. Toto ministerstvo zřídilo Sekci krizového managementu a civilní

ochrany, jejíž součástí je i Odbor civilní ochrany obyvatelstva, mezi jeho činnosti spadají i úkoly spojené s KI.

4.3.8 Španělsko

Ve Španělsku nebylo po dlouhou dobu oblast kritické infrastruktury žádným způsobem řešena a zabezpečena. Až teprve v roce 2007 Státní bezpečnostní sekretariát (State Security Secretariat) schválil Národní plán pro ochranu kritické infrastruktury (Plan Nacional de Protección de las Infraestructuras Recenze), který definuje kritickou infrastrukturu jako: *„Zařízení, sítě, služby, fyzické prostředky a informační technologie, jejichž zničení nebo poškození by mělo vážný dopad na zdraví, bezpečnost nebo hospodářský blahobyt občanů, nebo efektivní fungování státních institucí a veřejné správy.“*[24] Tento plán krom jiného také obsahuje seznam 12 strategických kritických oblastí, kterými jsou:

- chemický průmysl,
- jaderný průmysl,
- výzkumná zařízení,
- mocenská centra,
- vesmír,
- energetika,
- telekomunikace,
- doprava,
- zásobování vodou,
- potraviny,
- finanční sektor,
- veřejné zdraví.

Španělská vláda byla později v roce 2007 vyzvána Kongresem k sestavení katalogu se seznamem prvků KI. Seznam byl vytvořen v průběhu 6 měsíců a obsahuje na 3500 zařízení,

[24] BRUNNER, E.; SUTER, M..: *International CIIP Handbook 2008/2009 – An Inventory of 25 National and 7 International Critical Information Infrastructure Protection Policies.* Zurich [online]. ETH Zurich - Center for Security Studies, 2008, 648 p. Dostupný z WWW: <http://se2.isn.ch/serviceengine/FileContent?serviceID =11&fileid=8EAC1DE9-1B8D-DA5B-93D7-4FC32E2415B2&lng=en>.

která se nacházejí v celém Španělsku. Tento katalog slouží také jako základ pro spolupráci s ostatními zeměmi EU v rámci EPCIP.

Spolupráce soukromého a státního sektoru probíhá převážně v rámci programu Informační společnost a telekomunikační analytické centrum (ENTER - The Information Society and Telecommunications Analysis Center). Úkolem tohoto programu je zajištění poskytování informací obyvatelstvu.

4.4 Shrnutí kapitoly

V této kapitole byl nastíněn přístup v oblasti kritické infrastruktury, a to jak na úrovni Evropské unie jako celku, tak také v jednotlivých zemích tohoto uskupení. Z předešlého textu lze velmi jednoznačně vysledovat, že téměř většina zemí EU vytipovala oblasti KI, dle doporučení Sdělení Radě a Evropskému parlamentu KOM/2004/0702. Grafický řehled oblastí KI v zemích EU je pak součástí příloh (viz. Příloha 3 Přehled oblastí KI v jednotlivých zemích EU).

Jedinou oblastí původního návrhu Komise, kterou téměř žádná země nezahrnula do svého seznamu kritické infrastruktury je nakládání s nebezpečnými odpady, výjimku tvoří pouze Německo a Španělsko.

Rozdílnost v rozložení odpovědnosti za kritickou infrastrukturu a její ochranu se v jednotlivých zemích také do značné míry liší. Některé země již přijaly i zákony týkající se kritické infrastruktury, jiné začínají s implementací do svých právních předpisů až nyní. Jednoduchý přehled odpovědných orgánů ve výše uvedených zemích je uvedena v Tabulka 4 Přehled odpovědných orgánů.

Tabulka 4 Přehled odpovědných orgánů [16, 20]

Země	Zodpovědný orgán SS	Poznámky
Finsko	Národní nouzová zásobovací agentura (NESA)	analyzuje rizika a hrozby, vtváří podmínky pro
	Finský telekomunikační regulační úřad (FICORA)	
	Řídící výbor pro bezpečnost dat ve státní správě (VAHTI)	bezpečnsot informačních systémů
Francie	Generální tajemník pro národní obranu (SGDN)	oblast národní a mezinárodní bezpečnostní politiky
	Ústřední ředitelství bezpečnosti informačních systémů	úkoly spojené s ochranou KI
	Ministerská komise pro bezpečnost	
Maďarsko	Aktuálně se řeší odpovědnost za oblast KI	
Německo	Spolkové ministerstvo vnitra	
	meziresortní pracovná skupina AG KRITIS	
Nizozemí	Ministerstvo vnitra	
	Generální zpravodajská a bezpečnostní služba	
Norsko	Ministerstvo spravedlnosti a policie	zodpovidá za koordinaci v oblasti KI
	Ministerstvo pro záležitosti vlády a reformy	celková zodpovědnost za oblast KI
	Ministerstvo obrany	zodpovědnost za otázky obrany
Slovensko	Ministerstvo vnitra	odbor civilní ochrany obyvatelstva
Španělsko	Ministerstvo vnitra	
	Ministerstvo průmyslu, turistiky a obchodu	
Velká Británie	Ministerstvo vnitra	spolupráce se dalšími ministerstvy
	Centrum pro ochranu Národní Kritické Infrastruktury	spolupráce se soukromým sektorem

5 ČR a kritická infrastruktura

O problematice kritické infrastruktury se v Česku začíná hovořit v několika posledních letech. Toto má souvislost především s vytvářením dokumentů ve strukturách, kterých je Česká republika členem, především pak v NATO a Evropské unii. K poměrně rychlému vývoji v této oblasti, pak přispěli především útoky teroristů na evropská města.

Jedním z prvních odborných počinů na téma kritické infrastruktury byla konference Ochrana obyvatel 2007 pořádána VŠB – TU Ostrava, Fakultou bezpečnostního inženýrství a Sdružením požárního a bezpečnostního inženýrství, s názvem Ochrana kritické infrastruktury. Na této konferenci bylo předneseno několik příspěvků, a to jak odborníky z praxe, tak také akademickými pracovníky, právě na téma kritické infrastruktury.

Česká republika již podnikla několik kroků v dané oblasti, spočívajících především ve stanovení základních funkcí států v době krizových situací, vymezení přehledů subjektů kritické infrastruktury apod.

Česko také deklaruje, že hlavní úlohu musí převzít stát, neboť ten má za povinnost chránit zdraví, životy, majetek obyvatel, a životní prostředí. Avšak, krom státu musí být při řešení koncepce v oblasti KI přizvány i provozovatelé a majitelé jednotlivých prvků, neboť ti nejlépe vědí, jaké hrozby mohou ovlivnit jejich činnost, a stát také nemůže nést veškeré finanční náklady

5.1 Legislativa v oblasti KI

V současné době v ČR neexistuje konkrétní právní předpis, který by upravoval oblast kritické infrastruktury. Jediným současně závazným právním předpisem, je tedy Směrnice Rady 2008/114/ES ze dne 8. prosince 2008 o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu. Tento dokument je podrobněji popsán v části 4.2 Současné pojetí KI. Tato Směrnice ukládá členským zemím EU zapracovat její ustanovení do právních řádů, a to nejpozději do ledna roku 2011.

V oblasti legislativy se aktuálně připravuje novela zákona č. 240/2000 Sb., o krizovém řízení, ve znění pozdějších předpisů, přičemž novelizované znění by mělo obsahovat právě ustanovení Směrnice Rady, a mělo by také nově definovat zodpovědnost státních orgánu za přípravu k ochraně KI.

Do doby než bude novela přijata a začleněna do právního řádu, mohou být v souvislosti s kritickou infrastrukturou, alespoň částečně, použity stávající zákony z oblasti krizového řízení. Jedná se především o tzv. balíček krizových zákonů:

- z. č. 239/2000 Sb., o integrovaném záchranném systému, ve znění pozdějších předpisů, [13]
- z.č. 240/2000 Sb., o krizovém řízení, ve znění pozdějších předpisů, [12]
- z.č. 241/2000 Sb., o hospodářských opatřeních pro krizové stavy, ve znění pozdějších předpisů.

Dále také mohou být použity zákony upravující činnosti v jednotlivých odvětvích jako je energetika, vodní hospodářství, státní správa, apod. Jednalo by se především o:

- z.č. 458/2000 Sb., o podmínkách podnikání a o výkonu státní správy v energetických odvětvích (energetický zákon), ve znění pozdějších předpisů,
- z.č. 18/1997 Sb., atomový zákon, ve znění pozdějších předpisů,
- z.č. 254/2001 Sb., vodní zákon, ve znění pozdějších předpisů,
- z. č. 189/1999 Sb., o nouzových zásobách ropy, ve znění pozdějších předpisů
- vyhlášku č. 219/2001 Sb., o postupu v případě hrozícího stavu nouze v elektroenergetice, ve znění pozdějších předpisů,
- vyhlášku č. 225/2001 Sb., postup při vzniku a odstraňování stavu nouze v teplárenství, ve znění pozdějších předpisů,
- vyhláška č. 334/2009 Sb., o stavech nouze v plynárenství, ve znění pozdějších předpisů,
- a další.

Potřebu legislativních změn, je možné vnímat z několika pohledů Předně se je potřeba vymezit co je to kritická infrastruktura, a kdo a jakým dílem zodpovídá za opatření vedoucí ke zvýšení její ochrany. Zákon by měl krom jiného, dle mého názoru, obsahovat také práva a povinnosti provozovatelů a majitelů na straně jedné, a státu, respektive ministerstev a ÚSU v rámci jejich působnosti, na straně druhé. Velmi důležitým aspektem v oblasti ochrany kritické infrastruktury, je finanční stránka přijímaných opatření. Proto je potřeba pevně nastavit i pravidla v oblasti financování OKI. Je zcela zřejmé, že o finanční náklady se musí

dělit stát a soukromý sektor., poměr financování by měl být předmětem dalších jednání mezi státem a vlastníky (provozovateli) prvků KI.

5.2 Součástí národní kritické infrastruktury

Na základě usnesení BRS č.3/2007 bylo vybráno celkem 9 oblastí s 39 prvky, které považujeme za českou kritickou infrastrukturu. To znamená, že jejich výpadek či zničení by měly nepříznivý dopad na zdraví, životy, majetek obyvatel, životní prostředí, či zachováni základních funkcí státu. Přehled oblastí, prvků a odpovědných odborných gestorů je uveden v Tabulka 5 Přehled KI v ČR. Základní funkce státu jsou definovány jako: „*Činnosti státních orgánů, které jsou nutné k zajištění svrchovanosti, územní celistvosti, demokratických základů a mezinárodních závazků státu, práv a svobod občanů, jejich životů a zdraví, vnitřní bezpečnosti a veřejného pořádku, majetkových hodnot a životního prostředí.*“[25]

A jaký je vztah mezi základními funkcemi státu a kritickou infrastrukturou? Právě prostřednictvím prvků kritické infrastruktury, stát v případě krizových situací, naplňuje své základní funkce.

Je důležité také zmínit, že každý prvek kritické infrastruktury se skládá ze samostatných subjektů a objektů. Například prvek kritické infrastruktury *Elektřina* se skládá z dalších součástí jako: výroba el. energie, přenos energie (z elektráren), distribuce energie (vysoké a nízké napětí) a dispečerská centra. Každá z těchto součástí je tvořena subjekty KI (ČEZ, E.ON, PRE, ČEPS,…), které provozují jednotlivé objekty KI (elektrárny, sítě velmi vysokého, vysokého a nízkého napětí, rozvodné stanice, trafo stanice,…). Samozřejmě i u dalších prvků lze najít obdobné spojitosti.

V současné době by tedy snaha státu měla spočívat ve vytipování těchto součástí každého prvku a určení, subjektů a objektů KI. Dalším krokem, by pak logicky, mělo být navázání užší spolupráce se subjekty, které budou určeny, podrobné zmapování jednotlivých objektů a případné označení klíčových míst těchto objektů (místa jejichž vyřazení či poškození mohou mít vliv na danou část KI). Autor si je samozřejmě vědom, že u některých objektů (jako např. liniové stavby), jsou tyto činnosti jen obtížně proveditelné, a to především s ohledem na rozsáhlost těchto objektů.

[25] Terminologický slovník – krizové řízení a plánování obrany státu. Dostupný z WWW: <www.mvcr.cz>.

Tabulka 5 Přehled KI v ČR [18]

Oblast KI	Prvky KI	Gestor
Energetika	Elektřina	MPO
	Plyn	MPO
	Tepelná energie	MPO
	Ropa a ropné produkty	SSHR/MPO
Vodní hospodářství	Zásobování pitnou a užitkovou vodou	MZe
	Zabezpečení a správa povrchových vod a podzemních zdrojů vody	MZe/MŽP
	Systém odpadních vod	MZe
Potravinářství	Produkce potravin	MZe
	Péče o potraviny	
	Zemědělská výroba	
Zdravotní péče	Přednemocniční neodkladná péče	MZ
	Nemocniční péče	
	Ochrana veřejného zdraví	
	Výroba, skladování a distribuce léčiv a zdravotnických prostředků	
Doprava	Silniční	MD
	Železniční	
	Letecká	
	Vnitrozemská vodní	
Komunikační a informační systémy	Služby pevných telekomunikačních sítí	MPO/ČTÚ
	Služby mobilních telekomunikačních sítí	
	Radiová komunikace a navigace	
	Satelitní komunikace	
	Televizní a rádiové vysílání	
	Poštovní a kurýrní služby	
	Přístup k internetu a k datovým službám	MV
Bankovní a finanční sektor	Správa veřejných financí	MF
	Bankovnictví	ČNB
	Pojišťovnictví	
	Kapitálový trh	
Nouzové služby	Hasičský záchranný sbor ČR a příslušné JPO	MV
	Policie ČR (vnitřní bezpečnost a veřejný pořádek)	
	Armáda ČR (zabezpečení obrany)	MO
	Radiační monitorování vč. Podkladů pro rozhodování o opatřeních vedoucích ke snížení nebo odvrácení ozáření	SÚJB
	Předpovědní, varovná a hlásná služba	MŽP
Veřejná správa	Státní správa a samospráva	MV
	Sociální ochrana a zaměstnanost (sociální zabezpečení, stát. soc. podpora, soc. pomoc)	MPSV
	Výkon justice a vězeňství	MS

5.2.1 Subjekty kritické infrastruktury

Obecně lze subjekty kritické infrastruktury rozdělit podle následných kriterií:

1. **nenahraditelnost** – subjekt, činnost daného prvku nelze nahradit v krátkém časovém období, při výpadku je předpoklad vyhlášení krizových stavů, stavu nouze, regulačních stupňů, a to i pro území celého státu,
2. **nahraditelnost** – subjekt nebo činnost lze nahradit, a to v dostačují míře kvality; stavy nouze, krizový stav či regulační stupně mohou (ale nemusejí) být vyhlášeny v omezené míře (předpokládá se pouze na postiženém území),
3. **působnost** – rozdělení podle rozsahu jejich působnosti na místní, krajské, celostátní a nadnárodní subjekty (evropská KI).

Podle předchozích kriterií pak subjekty můžeme zařadit do 4 kategorii:

- I. kategorie – zařazení na základě kritéria 1 a 2, subjekty s celostátní působnosti,
- II. kategorie – subjekty s krajskou působností,
- III. kategorie – subjekty místní působnosti,
- Zvláštní kategorie – subjekty evropské KI.

Důležitým faktorem v oblasti ochrany kritické infrastruktury je oblast finančních nákladů, vynaložených na zabezpečení potřebných opatření. Je potřeba si uvědomit, že převážná většina subjektů KI jsou soukromé subjekty, které svou činnost vykonávají za účelem zisku, a minimalizace ztrát. A samozřejmě je z jejich strany požadavek, že finance jimi vynaložené se musejí vrátit. Všeobecně je známo, že prostředky, které budou vynaloženy na ochranu mají jen malou návratnost, a je jisté že subjekty nebudou chtít v takovém to prostředky vynakládat. Úkolem státních institucí, je vést se subjekty dialog, a přimět je aby finance v rozumné míře vynaložily, neboť dojde-li k poškození následkem mimořádných událostí či krizových situací, pak bude obnova jednodušší, rychlejší a především levnější, než kdyby finance nyní nevynaložily. Tato situace vychází i z postoje Komise, který zakazuje jakékoliv zvýhodňování různých průmyslových odvětví na úkor jiných. V praxi to tedy znamená, že stát, ač by sebe více chtěl, nesmí soukromému sektoru poskytovat finanční prostředky, neboť by tak došlo ke zvýhodnění dané subjektu.

Také je potřeba, aby požadavky na ochranu, které budou státem stanoveny, byly nejprve se subjekty konzultovány, neboť tak bude mít stát garantováno, že opatření budou subjekty

přijata a především pak implementována. Neboť opatření, která jsou státem nařízena, ale subjekty nerealizována, nemají v případě vzniku krizové situace žádný význam, a jak stát tak i subjekty musí vyvinout mnohem větší úsilí ke zvládnutí nastalé situace, což ve výsledku opět znamená zvýšení nákladů.

5.2.2 Objekty kritické infrastruktury [23]

Za objekty KI označujeme stavby a zařízení, které jsou provozovány subjekty kritické infrastruktury. Tyto objekty můžeme rozdělit podle několika kriterií, jako například velikosti postiženého území či dopadů na jiné objekty.

Podle velikosti postiženého území rozlišujeme:

1. objekty národního významu – vyřazení nebo narušení těchto objektů by mělo významný dopad na ekonomiku, činnosti veřejné správy, oblast bezpečnosti státu a zabezpečení základní potřeb obyvatelstva. Následky spojené s vyřazením těchto objektů by byly pravděpodobně řešeny jak jejich vlastníky, tak také ministerstvy a jinými ÚSÚ, v gesci jejich působnosti.
2. objekty místního (krajského) významu – poškození či vyřazení by mělo dopad na zachování funkcí území. Lze předpokládat, že následky spojené s výpadkem těchto prvků by museli řešit sami provozovatelé, v úvahu přichází ještě spolupráce s orgány kraje, či krajským HZS.

Podle dopadů na jiné oblasti lidské činnosti, pak rozlišujeme tři kategorie objektů:

1. prioritní – narušení těchto objektů má vliv i na činnosti jiných KI, nahraditelnost těchto prvků je jen velmi obtížná. Mezi prioritní objekty pak můžeme zařadit především energetické objekty, objekty komunikačních a informačních systémů, dopravní stavby, či takové prvky, jenž jsou svou funkcí jedinečné,
2. ostatní – při jejich výpadku dojde k narušení společenského života, ale jejich činnost je možné přijetím zvláštních opatření či využitím nouzových služeb nahradit. To této kategorie se mohou zařadit dodávky ropy a jejich produktů, zásobování vodou a potravinami, oblast zdravotnictví, bankovnictví čí státní správy – tyto prvky je právě možno do určité míry nahradit, či přijmout opatření k redukci ohrožení (náhradní zdroje energií, nouzové zásobování vodou, …),

3. zvláštní – takové objekty, jejich výpadek naruší společenské funkce jen při specifických situacích, jako jsou mimořádné události či krizové situace. Sem můžeme zařadit připravenost složek IZS, nouzových služeb, obrannou infrastrukturu.

V ČR jsou dále dle směrnice Ministerstva obrany[26] vymezeny objekty důležité pro obranu státu (ODOS) a objekty možného napadení (OMN). Jako ODOS označujeme pozemky, stavby a další objekty strategického významu, jejichž poškozením, částečným nebo celkovým zničením, případně neutralizací by nepřítel získal zjevné vojenské výhody a narušil by tím obranu státu. Oproti tomu OMN jsou pozemky a stavby, které při zajišťování obrany státu nemají strategický význam, ale na území správních obvodů krajů a obcí mají význam zásadní. Jedná se například o budovy územních samospráv, zdroje pitné vody, nemocnice, civilní letiště, mosty nebo velkosklady potravin.

5.3 Současné východiska

Jak bylo zmíněno výše do doby uzákoněni problematiky kritické infrastruktury, mohou být uplatňovány jiné zákonné normy, které jsou v současné době platné. Jedním ze současných přístupů v této oblasti může spatřovat v nastaveném systému krizového řízeni, podle již uvedeného zákona č. 240/2000 Sb.

Tento zákon upravuje působnost a pravomoc státních orgánů a orgánů územních samosprávných celků, práva a povinnosti právnických a fyzických osob při přípravě a řešení krizových situací, které nesouvisejí se zajišťováním obrany České republiky před vnějším napadením. Případné vojenské ohrožení státu je řešeno v zákoně č. 222/1999 Sb., o zajišťování obrany České republiky.

Krizové řízení je definováno jako: *„Souhrn řídících činností věcně příslušných orgánů zaměřených na analýzu a vyhodnocení bezpečnostních rizik, plánování, organizování, realizaci a kontrolu činností prováděných v souvislosti s řešením krizové situace.“*[27]

Systém krizového řízení lze rozdělit do tří úrovní:

1. místní – tvořena místní samosprávou (obce s rozšířenou působností, starostové ORP),

[26] Ministerstvo obrany ČR: *Směrnice k výběru objektu obranné infrastruktury a zpracování dokumentace*. Praha, 2007.

[27] Zákon č. 240/2000 Sb., o krizovém řízení a změně některých zákonů (krizový zákon), ve znění pozdějších předpisů

2. regionální – tvořena samosprávou vyšších územně správních celků (krajské úřady, magistrát hl.m. Prahy, hejtmani a primátor Prahy),
3. celostátní – tvořena vládou, ministerstvy a ústředními správními úřady.

Orgány krizového řízení vytváření i tzv. krizově plánovací dokumentaci, mezi kterou patří krizové plány, havarijní plány, typové plány, a také plány právnických a podnikajících fyzických osob – vnitřní havarijní plány, plány akceschopnosti, plány krizové připravenosti. Tato dokumentace je vytvářena za účelem, popsání rizik na daném území, a případného zmírnění a rychlého odstranění dopadů vzniklých mimořádných událostí či krizových situací. Právě tyto dokumenty mohou sloužit jako podklady pro případné plánování v oblasti ochrany kritické infrastruktury.

5.3.1 Krizové plány

Krizové plány jsou výstupem krizového plánování u orgánů krizového řízení a obsahují souhrn krizových opatření a postupů k řešení krizových situací.

Krizový plán se dělí na základní a přílohovou část. Základní část obsahuje informace o působnosti, odpovědnosti a úkolech orgánu krizového řízení, výčet a hodnocení možných krizových rizik, činnosti subjektů krizové řízení. V přílohové části jsou uváděny dokumenty nezbytné k zvládnutí nastalé situace (přehledy sil a prostředků, plány nezbytných dodávek, plány hospodářské mobilizace, plány akceschopnosti, povodňové plány, havarijní plány, topografické mapy apod.).

Tabulka 6 Přehled krizových plánů uvádí, jaké plány jsou na území ČR zpracovávány a kdo je jejich zpracovatelem.

Tabulka 6 Přehled krizových plánů [17]

	Typ dokumnetu	Zpracovatelé KP
Celostátní úroveň	Krizový plán správních úřadů	Ministerstva
		Ústřední správní úřady
		další státní orgány (dle § 28 odst. 2 zákona č. 240/2000 Sb.)
Regionální úroveň	Krizový plán kraje	Hasičský záchranný sbor kraje
Místní úroveň	Vybrané úkoly krizového plánu kraje (krizový plán určené obce)	Obce určené HZS kraje k rozpracování krizového plánu kraje

Kromě výše popsaných plánu a jejich zpracovatelů, existují také tzv. plány krizové připravenosti a plány akceschopnosti. Tyto dokumenty jsou zpracovány právnickými a

podnikajícími fyzickými osobami, které na základě výzvy orgánu krizového řízení plní opatření vyplývající z krizového plánu. Plán krizové připravenosti především upravuje přípravu dané osoby k řešení krizových stavů – působnost organizace navenek. Činnosti osoby směřující dovnitř organizace se pak plánují formou plánu akceschopnosti. Plán akceschopnosti upravuje činnosti vedoucí k zajištění připravenosti a pohotovosti k plnění krizových opatření.

Základními právními normami v oblasti krizového plánování jsou:

- zákon č. 240/2000 Sb., krizový zákon,
- nařízení vlády č. 462/2000 Sb., ve znění nařízení vlády č. 36/2003 Sb.

5.3.2 Havarijní plány

Havarijní plány jsou výstupem tzv. havarijního plánování. Havarijní plány obsahují opatření a postupy k provádění nezbytných záchranných a likvidačních prací na území postiženém mimořádnou událostí.

Rozlišujeme tři základní druhy HP:

1. Havarijní plány správních území – sem řadíme havarijní plány kraje, který zpracovává HZS kraje, pro území kraje. Vytváří se pro ty události, u nichž se předpokládá vyhlášení třetího nebo zvláštního stupně poplachu, dle poplachového plánu IZS.
2. Zonální havarijní plány – nebo také tzv. vnější havarijní plány. Tyto se zpracovávají pro území v okolí nebezpečného objektu (chemická a jaderná zařízení), a zpracovatelem je HZS kraje. Zóna havarijního plánování (zóna, v níž se plánují ochranná opatření) je v případě chemických zařízení určena krajským úřadem (na základě provedené analýzy podkladů poskytnutých provozovatelem), u objektů s ionizujícím zářením pak SÚJB.
3. Objektové havarijní plány – tzv. vnitřní havarijní plány. Zpracovává je provozovatel zařízení (chemické zařízení a zařízení s ionizujícím zářením) pro území podniku.

HP se člení do tří samostatných částí, a to *informační* (obsahuje údaje o zpracovateli, informace o území, analýzu rizik, očekávané dopady apod.), *operativní* (přehledy sil a prostředků, úkoly správních úřadů, kritéria pro vyhlášení krizových stavů, …) a plány *konkrétních činností* (plány popisující jednotlivé činnosti vykonávané v rámci záchranných a likvidačních prací).

Základními právními předpisy v oblasti havarijního plánování pak jsou:

- zákon č. 239/2000 Sb., o IZS,
- zákon č. 18/1997 Sb., atomový zákon,
- zákon č. 59/2006 Sb., zákon o prevenci závažných havárií,
- vyhláška č. 328/2001 Sb., o některých podrobnostech zabezpečení IZS,
- vyhláška č. 103/2006 Sb., o stanovení zásad pro vymezení zóny havarijního plánování a o rozsahu a způsob zpracování vnějšího havarijního plánu,
- nařízení vlády č. 11/1999 Sb., o zóně havarijního plánování,
- a další.

Mezi vnitřní havarijní plány pak můžeme zařadit i dokumenty zpracovávané podle dalších předpisů, především dokumentaci zdolávání požárů, dokumentace provozovatelů energetických zařízení pro řešení stavu nouze v energetice, případně plány ohrožení kvality povrchových a podzemních vod.

5.3.3 Typové plány

Tyto plány jsou zpracovávány ústředními správními úřady v gesci jejich působnosti. ÚSU zpracovávají typové plány pro 23 typových krizových situací, dle usnesení bezpečnostní rady státu č. 295/2002. Celkem je zpracováno 24 typových plánů, které obsahují, zásady, opatření, síly a prostředky pro řešení oněch 23 krizových situací.

Po obsahové stránce lze plány rozdělit do tří částí:

1. hodnocení situace – popis dané krizové situace (původci či příčiny vzniku, scénáře vývoje), dopady situace, podmínky a překážky řešení (a to včetně vazby na KI),
2. záměry řešení – popis typových zásad, postupů a opatření pro řešení nastalé situace a to v období: hrozby vzniku, bezprostřední hrozby vzniku, vzniku krizové situace, řešení a likvidace nastalé události,
3. údaje o zpracovateli – informace o odpovědných osobách za zpracování a aktualizaci plánů.

Souhrnný přehled typových plánů a orgánů státní správy, které jsou zodpovědné za jejich zpracování je součástí příloh této práce (Příloha 4 Přehled typových plánů).

5.4 Mimořádné události s dopadem na KI

Dělení mimořádných událostí existuje několik, vždy záleží na kritériích, podle kterých k rozdělení dochází. Tyto kriteria mohou být například rozsah, způsob vzniku, dopady na zdraví a životy obyvatel, majetek, životní prostředí, apod.

Nejčastěji se však setkáme s rozdělením podle činitelů, kteří způsobují jednotlivé mimořádné události. Toto rozdělení pak bývá následující:

a. **antropogenní mimořádné události,**
b. **naturogenní mimořádné události,**
c. **terorismus.**

Často se také můžeme setkat s tím, že terorismus je zařazován mezi antropogenní mimořádné události, neboť hlavním činitelem je člověk.

5.4.1 Antropogenní mimořádné události

Jedná se o ty druhy události, které jsou vyvolané člověkem, nebo činností, kterou koná. Mezi AMU spadají poruchy na výrobních zařízeních, havárie, dopravní nehody s únikem nebezpečných látek, či organizovaný zločin. Tyto mimořádné události můžeme rozdělit do tří podskupin:

- technogenní MU – provozní havárie, a havárie spojené s infrastrukturou,
- sociogenní
    - *vnitřní* – negativní jevy v oblastech jako vnitřní pořádek státu, sociální a ekonomické sféře,
    - *vnější* – do této skupiny pak řadíme mezinárodní vztahy států, válečné konflikty, apod.,
- agrogenní – někdy také označovány jako kombinované (činiteli jsou částečně člověk a částečně přírodní síly), souvisejí s přeměnou půdy pro její hospodářské využití.

V souvislosti s kritickou infrastrukturou a jejím ohrožením, jsou největší hrozbou, události které mají rychlý vývoj a je jen velmi těžké je s dostatečným předstihem předvídat. Lze konstatovat, že nejnebezpečnější v této kategorii jsou průmyslové havárie,či havárie při dopravě nebezpečných látek, neboť může dojít k ohrožení hned několika prvků kritické infrastruktury. Jsou-li látky přepravovány, vyráběny či skladovány v zastavěných oblastech,

pak může při havárii dojít k ohrožení prvků z oblasti zdravotnictví, veřejné správy, vodního hospodářství či potravinářství. Je zřejmé, že při výpadku těchto prvků může dojít k návazným výpadkům v dalších oblastech.

5.4.2 Naturogenní mimořádné události

Události, které jsou vyvolány přírodními vlivy a zákonitostmi přírody. Naturogenní mimořádné události, lze rozdělit do dvou podskupin, a to podle toho zda jsou způsobeny neživými (abiogenní) či živými (biogenní) složkami přírody.

Události, které mohou na území České republiky způsobit rozsáhlé škody, a tím být nebezpečné i pro samotnou kritickou infrastrukturu, jsou:

- povodně a záplavy,
- vichřice a jiné atmosférické jevy,
- požáry,
- sesuvy půdy,
- epidemie, epizotie,
- zemětřesení, a jiné.

Území republiky je v posledních několika letech, téměř každý rok postihováno, některou z výše popsaných naturogenních mimořádných událostí. Z posledních událostí, které naše území zasáhly, by bylo možno zmínit povodně v létě roku 2009, či silné větrné smršť. Během těchto událostí, bylo postiženo území hned několika krajů České republiky, a způsobily problémy v mnoha oblastech. Především pak v dopravě, zásobování energiemi, vodou a potravinami, ale také v oblastech státní správy, neboť bylo poškozeno mnoho úředních budov, a tedy nebylo možné poskytovat plně všechny činnosti. Samozřejmě, takovéto události dopadají i na havarijní složky, které musejí následky MU odstraňovat. A v neposlední řadě, je dopad citelný i v oblasti veřejných financí, jelikož stát musí vynaložit finance na obnovu poškozené infrastruktury, jako jsou cesty či budovy.

5.4.3 Terorismus

Jak již bylo napsáno výše, terorismus je často řazen mezi antropogenní mimořádné události, neboť jeho činiteli či původci jsou lidé. Avšak je zde značný rozdíl v tom, že terorismu je záměrná činnost člověka, s primárním cílem škodit, kdežto jiné antropogenní MU pak vznikají většinou z neopatrnosti či zanedbání povinnosti. Samozřejmě i další socio-patogenní

činnosti (organizovaný zločin, drogové závislosti, protiprávní činnosti), které řadíme mezi antropogenní MU, jsou škodlivé. Terorismu se oproti nim vyznačuje tím, že jeho činnost je směřována vůči široké veřejnosti, a tím je vyvíjen tlak na oficiální představitele států, aby teroristům ustoupili, a ti tak dosáhli svých cílů.

Z mého pohledu je největší hrozbou terorismu fakt, že je jen velmi složité odhalit spletitou síť teroristických organizací, a tím i velmi těžké, lze říct téměř nemožné zjištění doby a místa útoku. Navíc teroristé jsou lidé, kteří nejsou vázání žádnými předpisy, pravidly či zákony, a některé státy je dokonce chrání, či finančně nebo materiálně podporují. Tato podpora přetrvává i přes různé sankce, které mezinárodní společenství vůči těmto zemím uplatňuje.

K dosažení svých cílů používají teroristé nejrůznějších metod a praktik, jako jsou pumové atentáty, nástražné výbušné systémy, únosy lidí, útoky na sídla zastupitelských úřadů, apod. V současnosti jsou teroristy využívány pouze konvenční zbraně. Avšak dostanou-li se ke zbraním hromadného ničení (dále ZHN), jako jsou chemické, biologické či nukleární zbraně, pak musíme předpokládat, že se jejich užití nebudou zdráhat.

Nebezpečnost ZHN je možné vidět z několika pohledů. Především se jedná o oblast detekce těchto látek, a také ochrany před jejich účinky. V současné době jsme schopni detekovat přítomnost radiace a také mnoha chemických látek, avšak v oblasti biologických látek, je situace mnohem složitější, neboť expozice těchto látek se projeví až po uplynutí určité doby (inkubační doba), která může činit až několik dní. Navíc během této doby exponované osoby mohou sloužit jako zdroje nákazy, a do propuknutí příznaků nákazy dále šířit. Tím že je látka detekována, však vše teprve začíná, neboť jako následné opatření musí být státem zajištěna odpovídající ochrana, proti účinkům těchto látek a to jak obyvatelstvu, tak i složkám IZS a dalším osobám, které se podílejí na odstraňování následků, takto vzniklých událostí. Lze konstatovat, že jedinými složkami IZS, které jsou, alespoň částečně vybaveny ochrannými prostředky, jsou jednotky HZS a armády ČR, ostatní složky nemají ve svém vybavení, ani základní ochranné prostředky, jako jsou celoobličejové masky s odpovídajícími ochrannými filtry. Mimo oblasti detekce látek a ochrany proti účinkům, je pak dalším problémem i dekontaminace zamořených oblastí, přičemž tyto oblasti mohou být značně velké, s přihlédnutím na druh, kvalitu, množství použité látky, povětrnostní podmínky a mnoho dalších.

Zopakujme si nyní, jak teroristé chtějí dosáhnout svých cílu. Jejich snahou je poškození co největší masy obyvatel! Ano a právě kritická infrastruktura je v tomto ohledu velmi vhodným

cílem. Pokud dojde k poškození či vyřazení prvků KI, bude to mít v konečných důsledcích dopad právě na širokou veřejnost. Proto je možné předpokládat, že v budoucnu se teroristé na prvky kritické infrastruktury budou zaměřovat, mnohem více než tomu bylo doposud.

Za oblasti, které by si teroristé mohli vybrat jako své cíle, bych zařadil odvětví energetiky, telekomunikací, státní správy. Neboť vyřazení těchto struktur, by mělo velmi významný dopad na funkčnost celého státu. Velkou váhu má právě oblast komunikací, neboť bez potřebných informací a prostředků komunikace, nelze v dostatečně míře řídit a koordinovat potřebné činnosti, k odstranění následků vzniklých situací.

6 Kritičnost prvků

Jedním z cílu této práce, které jsem si určil, je určení kritičnosti jednotlivých prvků kritické infrastruktury. K tomu účelu byla vybrána analýza souvztažnosti. Proč právě tato metoda? Jedná se o typ analýzy, která slouží k hledání a identifikaci vazeb mezi zdroji a objekty rizik.

Kritičnost jako taková může mít několik podob. Kritičností pro účely této práce rozumíme vzájemné vazby a vztahy mezi jednotlivými prvky kritické infrastruktury. Tedy kolik prvků může být ovlivněno výpadkem, vyřazením či zničením daného prvku, a naopak které z prvků mohou při své nefunkčnosti posuzovaný prvkem ovlivnit.

Při této analýze si klademe otázku: Může následkem výpadku, vyřazení či zničení prvku X (ve sloupci) dojít k výpadku, vyřazení či zničení prvku Y (v řádku). Obecně platí, že každý prvkem může ovlivnit prvek jiný, záleží však na tom, zda je o ohrožení primární či sekundární. V použité analýze posuzujeme pouze primární (přímá) ohrožení. Ta nastávají tehdy, dojde-li v souvislosti s vyřazením posuzovaného prvku, k bezprostřednímu ohrožení prvku druhého.

Příklad primárního ohrožení:
Dojde-li k vyřazení prvku Elektřina, pak s největší pravděpodobností, tato událost bude mít značný dopad na prvek Produkce potravin. Toto je dáno závislosti naší společnosti na elektrické energii, neboť téměř vše co člověk denně používá, ke svému fungování potřebuje elektřinu.

Příklad sekundárního ohrožení:
Bude-li vyřazen prvek Správa veřejných financí, nedojde k primárnímu ohrožení prvku Silniční doprava, neboť ta bude i nadále funkční, jelikož na tomto prvku není přímo závislá. Sekundární ohrožení zde představuje skutečnost, že stát jako správce komunikací nebude mít prostředky na jejich údržbu. Komunikace se mohou stát nesjízdnými a tato skutečnost může vést k výpadku Silniční dopravy.

6.1 Postup analýzy

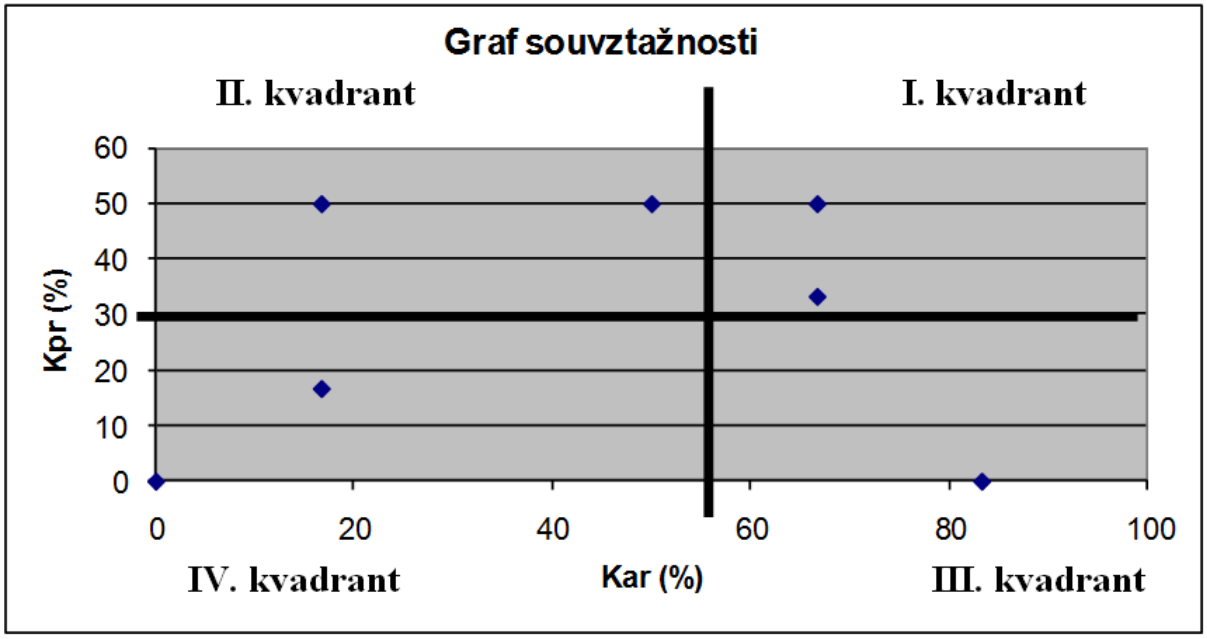
Postup při sestavování analýzy souvztažnosti jde rozdělit do 5 bodů, a to:

1. sběr dat a jejich zpracování,
2. hodnocení dat,

3. identifikace rizika – hodnotíme každý prvek systému s každým prvkem, pro hodnocení používáme hodnot 0 (NE) a 1 (ANO),
4. výpočet koeficientů K_{ar}, K_{pr},
5. vynesení dat do grafu, určení os O_1 a O_2, jenž nám vytvoří čtyři kvadranty.

Výsledkem analýzy je tedy matice rizik, ve které jsou přehledně uvedeny vzájemné souvislosti mezi jednotlivými prvky posuzovaného systému. Sloupce udávají, které prvky jsou posuzovaným prvkem ovlivněny, řádky pak jaké prvky nám posuzovaný prvek ovlivní.

Jak bylo zmíněno v bodu 5, výpočtem os X a Y, dojde k rozdělí na čtyři kvadranty, které nám určují míru rizika – I. kvadrant = primární rizika, II. kvadrant = sekundární rizika, III. kvadrant = žádná primární rizika, IV. kvadrant = relativní bezpečnost. Rozdělí kvadrantů v grafu je uvedeno níže (viz. Graf 1 Příklad grafu analýzy souvztažnosti).



Graf 1 Příklad grafu analýzy souvztažnosti [19]

6.2 Výpočty

Pro úspěšné dokončení vlastní analýzy je potřeba vypočítat celkem čtyři údaje, a to koeficienty K_{ar} (1) a K_{pr} (2), a osy O_1 (3) a O_2 (4).

Jednotlivé výpočty jsou provedeny dle následujících vzorců:

$$K_{ar} = \left(\frac{\sum K_{ar}}{x-1} \right) \cdot 100 \qquad (1)$$

$$K_{pr} = \left(\frac{\sum K_{pr}}{x-1} \right) \cdot 100 \qquad (2)$$

$$O_1 = 100 - \left(\frac{K_{ar\max} - K_{ar\min}}{100} \right) \cdot s \qquad (3)$$

$$O_2 = 100 - \left(\frac{K_{pr\max} - K_{pr\min}}{100} \right) \cdot s \qquad (4)$$

K_{ar}… procentní vyjádření počtu návazných rizik v řádku, které mohou být vyvolána rizikem jenž posuzujeme

K_{pr}…procentní vyjádření počtu vyvolaných rizik

x…počet hodnocených rizik

s…spolehlivost (0-100)

Konkrétní výpočty jsou z důvodu rozsáhlosti uvedeny v přílohách k této práci (viz. Příloha 5 Analýza souvztažnosti – výpočty). Hodnota spolehlivosti pro analýzu byla stanovena na 90%.

6.3 Výsledky analýzy

Provedenou analýzou souvztažnosti byla určena kritičnost jednotlivých prvků. Výstupem analýzy je graf souvztažnosti (viz. **Chyba! Nenalezen zdroj odkazů.**) a matice rizik (viz. Příloha 7 Matice rizik).

Následuje přehled prvků dle zařazení do jednotlivých kvadrantů.

I. kvadrant – dle výsledků analýzy nebyly určeny žádná primární rizika.

II. kvadrant – jakožto sekundární rizika byly určeny tyto prvky: Elektřina, Internet a data, a Ropa.

III. kvadrant – mezi žádná primární rizika pak patří Justice a vězeňství, Zásobování pitnou a užitkovou vodou, Armáda české republiky, Předpovědní a hlásná služba.

IV. kvadrant – do oblasti relativní bezpečnosti pak spadají ostatní prvky české KI.

I když některé prvky spadají do IV. kvadrantu, tedy jsou hodnoceny jako relativně bezpečná, je potřeba zmínit, že právě jejich výpadek by mohl mít zásadní vliv na další prvky a také

obyvatelstvo. Mezi tyto prvky bych zařadil Rádiovou komunikaci, Silniční dopravu, Správu veřejných financí a Policii ČR.

7 Závěr

Diplomová práce přináší základní informace o problematice kritické infrastruktury a její ochraně. Většina zemí si uvědomuje důležitost těch prvků infrastruktury, které jsou nezbytné k zachování základních funkcí státu a uspokojení potřeb obyvatelstva. Právě takovéto prvky pak jsou označovány jako kritická infrastruktura. Oblasti v jednotlivých zemích světa se mohou lišit. To, že se oblastí různí, je podmíněno především zvyklostmi, místními specifiky, uspořádáním struktury státní správy a v neposlední radě i zaměřením průmyslové výroby, té které země. Například ve Francii je jedním z odvětví KI oblast jaderného průmyslu, to je podmíněno skutečností, že Francie je zemí s dlouholetou tradicí tohoto odvětví, přičemž takových příkladů je možno najít několik.

Cílem diplomové práce bylo porovnat systémy kritické infrastruktury v členských zemích EU. K tomu aby byl celkový cíl naplněn, byly vytýčeny následné podružné cíle:

- vymezení kritické infrastruktury,
- popis přístupu k problematice ve světě,
- popis přístupu v EU a jejich zemích,
- kritická infrastruktura a ČR.

Jednotlivé cíle pak odpovídají kapitolám této práce.

Lze konstatovat, že většina, ne-li všechny země, se shodují na následujících oblastech kritické infrastruktury:

- energetika,
- potravinářství,
- zásobování vodou,
- zdravotnictví,
- doprava,
- komunikační a informační systémy,
- finanční sektor,
- a státní správa.

V České republice je celkem 9 oblastí s celkovým počtem 39 prvků kritické infrastruktury. Nelze však říci, že výpadek každého jednoho prvku by měl stejné následky. Mezi nejkritičtější prvky v České republice dle provedené analýzy pak spadají Elektřina, Internet a data, Ropa, Zásobování pitnou a užitkovou vodou, ale také Silniční doprava či ozbrojené a bezpečnostní sbory, včetně justice.

Proč právě tyto odvětví lidské činnosti? Odpověď poměrně jednoduchá, je to dáno skutečností, že výpadek, byť sebemenší má dopad na širokou veřejnost. Toto nám potvrzují i události z poslední doby, kdy následkem nepříznivých povětrnostních podmínek, byl nad téměř celou Evropou zastaven letecký provoz. Touto události bylo postiženo mnoho desítek tisíc osob.

Jaký je současný trend v oblasti kritické infrastruktury? Většina zemí se dnes snaží do svých právních řádů zanést důležitá ustanovení Směrnice Rady EU 2008/114/ES. Země si však uvědomují, že práce nekončí určením oblastí a prvků KI. Je nezbytně nutné začít věnovat pozornost i samotné ochraně takto vybraných prvků. Problémem v oblasti ochrany je fakt, že většina prvků je ve vlastnictví soukromého sektoru, přičemž ochranná opatření stojí nemalé finanční prostředky. Je tedy úkolem vlád, státních úřadů a vlastníku najít společnou řeč, v oblasti finančního zabezpečení ochrany kritické infrastruktury. Myslím, že právě hlubší spolupráce mezi soukromým sektorem a státem, bude hlavním směrem v oblasti problematiky kritické infrastruktury v následných letech.

Důležitým aspektem v oblasti kritické infrastruktury je samozřejmě i mezinárodní spolupráce. V tomto směru byly položeny základy jak na úrovni Evropské unie, tak také v prostředí Severoatlantické aliance. V rámci Evropské unie již několik let funguje Evropský program na ochranu kritické infrastruktury, jehož základním cíle je sdílení informací mezi členskými státy unie o možných rizicích, v jednotlivých odvětvích.

Přehled použitých zkratek

CEP	Civilní nouzové plánování (Civil Emergency Planning)
CIWIN	Varovná informační sít kritické infrastruktury (Critical Infrastructure Warning Information Network)
CPNI	Centrum pro ochranu Národní Kritické Infrastruktury (Centre for the Protection of the National Infrastructure)
ČEPS	Česká přenosová soustava
ČNB	Česká národní banka
EKI	Evropská kritická infrastruktura
EPCIC	Evropský program na ochranu kritické infrastruktury (European Programme for Critical Infrastructure Protection)
EU	Evropská Unie
FICORA	Finský telekomunikační regulační úřad (The Finnish Communications Regulatory Authority)
HZS	Hasičský záchranný sbor
IZS	Integrovaný záchranný systém
KI	Kritická infrastruktura
KP	Krizový plán
KS	Krizová situace
MD	Ministerstvo dopravy
MF	Ministerstvo financí
MPO	Ministerstvo průmyslu a obchodu
MS	Ministerstvo spravedlnosti

MU	Mimořádná událost
MV	Ministerstvo vnitra
MV - GŘ HZS	Ministerstvo vnitra - Generální ředitelství hasičského záchranného sboru
MZd	Ministerstvo zdravotnictví
MZe	Ministerstvo zemědělství
MŽP	Ministerstvo životního prostředí
NATO	Severoatlantická smlouva
NESA	Národní nouzová zásobovací agentura (National Emergency Supply Agency)
NISCC	Bezpečnostní Koordinační Centrum Národní Infrastruktury (National Infrastructure Security Co-ordination Centre)
NKI	Národní kritická infrastruktura
NSAC	Národní Poradenské Bezpečnostní Centrum (National Security Advice Centre)
ODOS	Objekty důležité pro obranu státu
OKI	Ochrana kritické infrastruktury
OMN	Objekty možného napadení
ORP	Obec s rozšířenou působností
PRE	Pražská energetika a.s.
SCEPC	Výbor pro civilní nouzové plánování (Senior Civil Emergency Planning Committee)
SGDN	Generální tajemník pro národní obranu (The Secretary general for National Defense)
SS	Státní správa

SSHR	Správa státních hmotných rezerv
SÚJB	Státní úřad pro jadernou bezpečnost
USA	Spojené státy americké
ÚSÚ	Ústřední správní úřady
VAHTI	Řídící výbor pro bezpečnost dat ve státní správě (Steering Committee for Data Security in State Administration)
VB	Velká Británie
ZHN	Zbraně hromadného ničení (někdy označovány jako CBRN)

Přehled použité literatury

Právní předpisy

[1] PUBLIC LAW 107–56—OCT. 26, 2001 UNITING AND STRENGTHENING AMERICA BY PROVIDING APPROPRIATE TOOLS REQUIRED TO INTERCEPT AND OBSTRUCT TERRORISM

[2] The National Strategy For Homeland Security, July 2002 [online]. Dostupný z WWW: <http://www.dhs.gov/xabout/history/publication_0005.shtm>

[3] National Strategy for Physical Protection of Critical Infrastructure and Key Assets [online]. Dostupný z WWW: <http://www.dhs.gov/files/publications/publication_0017.shtm>

[4] Komise Evropských společenství. Sdělení Komise Radě a Evropskému parlamentu. *Ochrana kritické infrastruktury při boji proti terorismu*. Brusel, 2004. KOM/2004/0702

[5] Komise Evropských společenství. *Zelená kniha o Evropském programu na ochranu kritické infrastruktury*. Brusel, 2005. KOM/2005/0576

[6] Komise Evropských společenství. *Sdělení Komise o Evropském programu na ochranu kritické infrastruktury*. Brusel, 2006. KOM/2006/0786

[7] Směrnice Rady EU. *O určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu.* 2008/114/ES

[8] Ministerstvo vnitra SR. *Koncepcia kritickej infraštruktúry v Slovenskej republike a spôsob jej ochrany a obrany* [on-line]. Bratislava, 2006. 19 s. Dostupné z WWW: <http://www.minv.sk>

[9] Ministerstvo vnitra SR. *Národní program pre ochranu a obranu kritickej infraštruktúry v Slovenskej republike* [on-line]. Bratislava, 2007. 24 s. Dostupné z WWW: <http://www.minv.sk>

[10] Vláda ČR. Usnesení vlády České republiky ze dne 25. února 2008 č. 165 k Vyhodnocení stavu realizace Koncepce ochrany obyvatelstva do roku 2006 s výhledem do roku 2015 a o Koncepi ochrany obyvatelstva do roku 2013 s výhledem do roku 2020. Praha, 2008

[11] Vláda ČR. Usnesení ze dne 25. února 2008 č. 170 o Harmonogramu dalšího postupu zpracování dokumentů Komplexní strategie České republiky k řešení problematiky kritické infrastruktury a Národního programu ochrany kritické infrastruktury. Praha, 2008

[12] Zákon č. 240/2000 Sb., o krizovém řízení, ve znění pozdějších předpisů [cit. 2010-02-12]

[13] Zákon č. 239/2000 Sb., o IZS, ve znění pozdějších předpisů [cit. 2007-02-12]

Publikace

[14] *NATO Handbook* [online]. Dostupný z WWW: <http://www.nato.int/docu/handbook/2001/index.htm#CH7>

[15] GORDON, K.; DION, M.: *PROTECTION OF 'CRITICAL INFRASTRUCTURE' AND THE ROLE OF INVESTMENT POLICIES RELATING TO NATIONAL SECURITY*. Paris : France : OECD, 2008. 11 s

[16] BRUNNER, E.; SUTER, M.: *INTERNATIONAL CIIP HANDBOOK 2008 / 2009 : AN INVENTORY OF 25 NATIONAL AND 7 INTERNATIONAL CRITICAL INFORMATION INFRASTRUCTURE PROTECTION POLICIES*. Series Editors: Andreas Wenger, Victor Mauer and Myriam Dunn Cavelty. Zurich, 2008. 546 s. Dostupný z WWW: <http://www.crn.ethz.ch>

[17] ŠENOVSKÝ, M.; ADAMEC, V.; VANĚK, M.: *Bezpečnostní plánování*. Ostrava : SPBI Spektrum, 2006. 86 s. ISBN 80-86634-52-4

[18] ŠENOVSKÝ, M.; ADAMEC, V.; ŠENOVSKÝ, P.: *Ochrana kritické infrastruktury*. Ostrava : SPBI Spektrum, 2007. 141 s. ISBN 978-80-7385-025-8

[19] ŠENOVSKÝ, M.; ADAMEC, V.: *Základy krizového managementu.* Ostrava : SPBI Spektrum, 2004. 102 s. ISBN 80-86634-44-2

[20] GAVENDOVÁ, H.: *KOMPARACE OCHRANY KRITICKÉ INFRASTRUKTURY V ČESKÉ REPUBLICE A EVROPSKÉ UNII*. [s. l.], 2009. 88 s. Masarykova univerzita Brno. Ekonomicko správní fakulta. Vedoucí diplomové práce Ing. Eduard Bakoš

Ostatní

[21] *Rozsah základních funkcí státu* (projekt), MV-GŘ HZS ČR, č.j.: PO-297-16/PLA-2002, usnesení Výboru pro civilní nouzové plánování č. 153 ze dne 24.9.2002, 7 s.

[22] Australian Goverment, Attorney-General's Department National Security Website. *Http://www.ag.gov.au* [online]

[23] MARTÍNEK, B.: *Východiska a principy zajištění ochrany kritické infrastruktury v České republice.* 112 – odborný časopis požární ochrany, integrovaného záchranného

systému a ochrany obyvatelstva. 2008, č. 4, s. 22. Dostupné na WWW: <http://web.mvcr.cz/archiv2008/casopisy/112/2008/duben/strana_ 22.html>.

[24] Commission for the Protection of Critical Infrastructures: *Protection of critical infrastructures and critical societal functions in Norway*. Norsko : [s.n.], 2006

WWW stránky

http://www.regjeringen.no

http://www.publicsafety.gc.ca

http://www.nesa.fi/

http://www.minbzk.nl

http://www.mvcr.cz

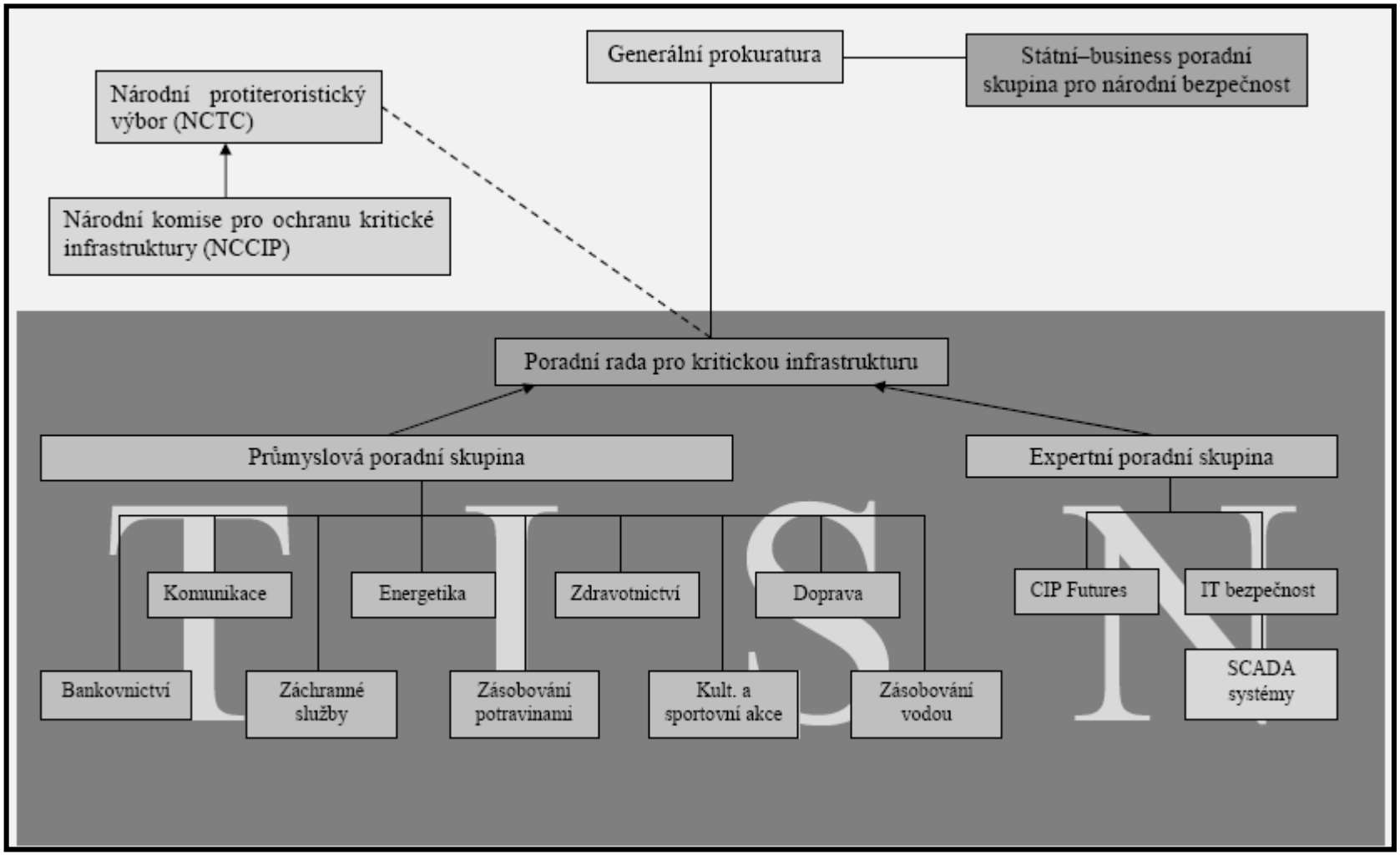
http://www.nato.int

http://www.minv.sk

Přílohy

Seznam příloh

Příloha 1 Systém ochrany KI v Austrálii

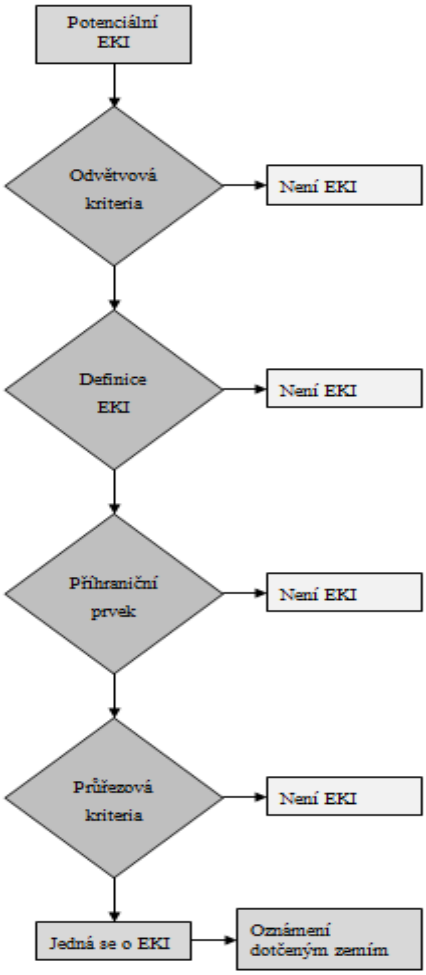


Příloha 2 Postup k určení EKI

Za evropskou kritickou infrastrukturu mohou být označeny pouze ty prvky a odvětví, jenž splňují kritéria dle následujících kroků.

1. Odvětvová kriteria – využijí se za účelem prvotního výběru infrastruktur v rámci daného odvětví.
2. Na prvky, které splnily podmínky dle kroku jedna se použije definice EKI.
3. Uplatnění příhraničního prvku podle čl. 2 písm. b. (u prvků zajišťující nezbytnou službu zohledňujeme možnosti alternativ a dobu trvání).
4. Uplatnění průřezových kriterií.

Potencionální EKI, které vyhověly dle předchozího postupu, musí členský stát ohlásit těm státům na než by mělo vyřazení závažný dopad.



Příloha 3 Přehled oblastí KI v jednotlivých zemích EU

	Původní návrh komise (2004)	Finsko	Francie	Maďarsko	Německo	Nizozemí	Norsko	Slovensko	Španělsko	Velká Britanie	ČR
Energetika	x	x	x	x	x	x	x	x	x	x	x
Informační a komunikační	x	x	x	x	x	x	x	x	x	x	x
Finančnictví	x	x	x	x	x	x	x	x	x	x	x
Zdravotnictví	x	x	x	x	x	x	x	x	x	x	x
Potraviny	x		x	x	x	x	x	x	x	x	x
Vodní hospodářství	x	x	x	x	x	x	x	x	x	x	x
Doprava	x	x	x	x	x	x	x	x		x	x
Nebezpečné látky	x				x				x		
Vláda, státní správa	x		x	x	x	x	x		x	x	x
Tisk		x									
Justice			x		x	x	x			x	x
Veřejný pořádek				x		x				x	
Průmysl			x	x				x	x		
Záchranné služby					x		x	x		x	x
Výzkum a vesmír			x		x				x		
Ozbrojené síly			x	x			x	x			

Příloha 4 Přehled typových plánů

Název typového plánu	Gestor
Dlouhodobá inverzní situace	MŽP
Povodně velkého rozsahu	MŽP
Jiné živelné pohromy velkého rozsahu	MV
Epidemie	MZd
Epifytie - hromadné nákazy polních kultur	Mze
Epizootie - hromadné nákazy zvířat	MZe
Radiační havárie	MV, SÚJB
Havárie velkého rozsahu způsobená vybranými nebezpečnými chemickými látkami s chemickými přípravky	MV
Jiné technické a technologické havárie velkého rozsahu - výbuch (exploze)	MV, GŘ-HZS
Narušení hrází významných vodohospodářských děl se vznikem zvláštní povodně	MZe
Znečištění vod, ovzduší a životního prostředí haváriemi velkého rozsahu nebude zpracován	
Narušení finančního a devizového hospodářství státu	MF, ČNB
Narušení dodávek ropy a ropných produktů velkého rozsahu	SSHR
Narušení dodávek elektrické energie, plynu a tepelné energie velkého rozsahu	MPO
Narušení dodávek potravin velkého rozsahu	MZe
Narušení dodávek pitné vody velkého rozsahu	MZe
Narušení dodávek léčiv a zdravotnického materiálu velkého rozsahu	MZd
Narušení funkčnosti dopravní soustavy velkého rozsahu	MD
Narušení funkčnosti veřejných telekomunikačních vazeb velkého rozsahu	MV
Narušení funkčnosti veřejných informačních vazeb velkého rozsahu	MV
Migrační vlny velkého rozsahu	MV
Hromadné postižení osob mimo epidemii, včetně hygienických režimů	MZd
Narušení zákonitosti velkého rozsahu	MV
Narušení funkčnosti poštovních služeb	MPO

Příloha 5 Analýza souvztažnosti – výpočty

Výsledné koeficienty K_{ar} a K_{rb}

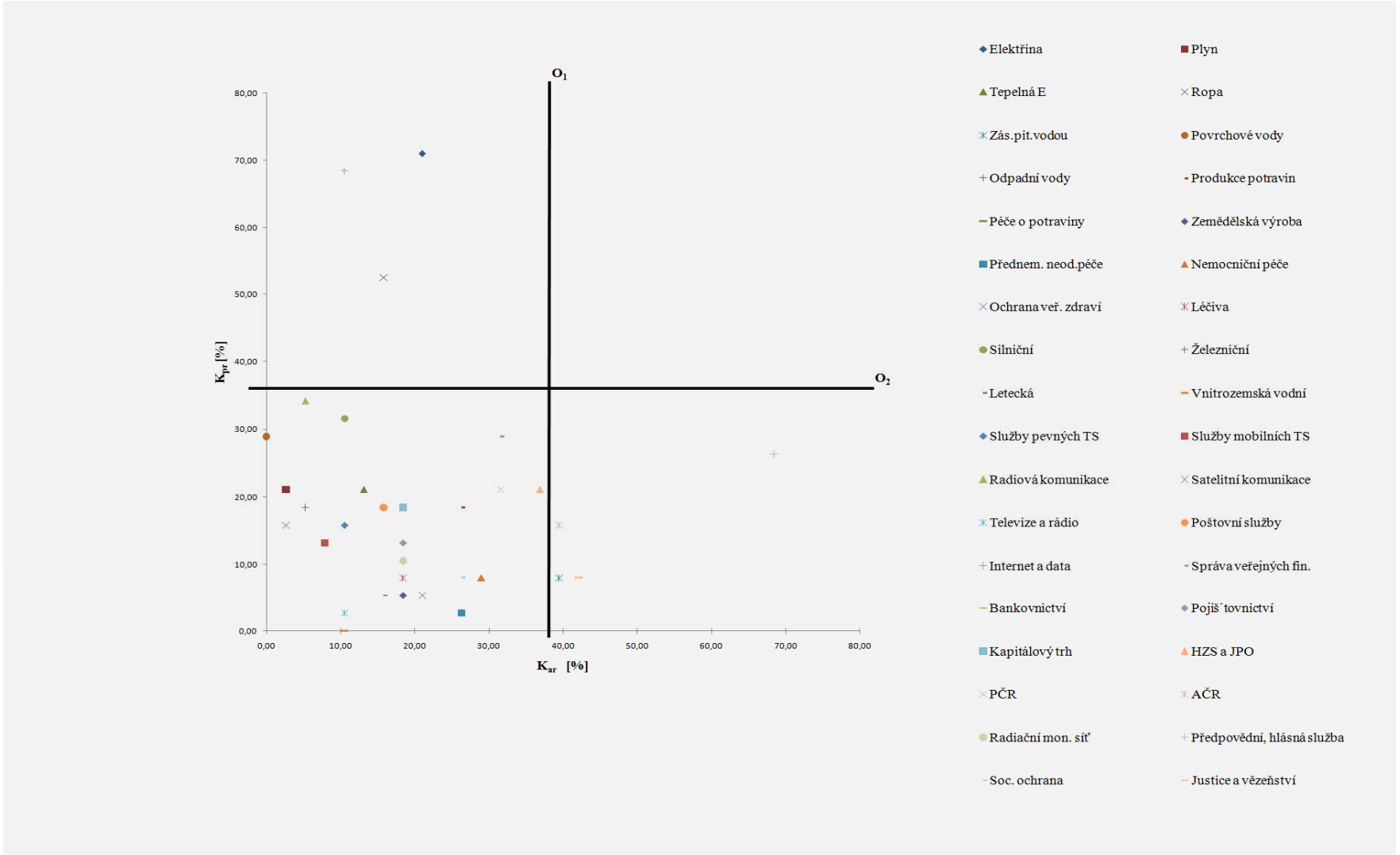
	ΣK_{ar}	ΣK_{rb}	K_{ar} [%]	K_{rb} [%]
Elektřina	8	27	21,05	71,05
Plyn	1	8	2,63	21,05
Tepelná E	5	8	13,16	21,05
Ropa	6	20	15,79	52,63
Zás. pit. a už. vodou	3	15	7,89	39,47
Povrchové vody	0	11	0,00	28,95
Odpadní vody	2	7	5,26	18,42
Produkce potr.	10	7	26,32	18,42
Péče o potr.	7	2	18,42	5,26
Zem. výroba	7	2	18,42	5,26
Přednem. neod.péče	10	1	26,32	2,63
Nemocniční p.	11	3	28,95	7,89
Ochr. veř. zdraví	8	2	21,05	5,26
Léčiva	7	3	18,42	7,89
Silniční	4	12	10,53	31,58
Železniční	4	6	10,53	15,79
Letecká	6	2	15,79	5,26
Vnitrozemská vodní	4	0	10,53	0,00
Služby pevných TS	4	6	10,53	15,79
Služby mobilních TS	3	5	7,89	13,16
Rádiová komunikace	2	13	5,26	34,21
Satelitní komunikace	1	6	2,63	15,79
Televize a rádio	4	1	10,53	2,63
Poštovní služby	6	7	15,79	18,42
Internet a data	4	26	10,53	68,42
Správa veřejných fin.	12	11	31,58	28,95
Bankovnictví	7	5	18,42	13,16
Pojištovnictví	7	5	18,42	13,16
Kapitálový trh	10	7	26,32	18,42
HZS a JPO	14	8	36,84	21,05
PČR	12	8	31,58	21,05
AČR	15	6	39,47	15,79
Radiační mon. síť	7	4	18,42	10,53
Předpovědní, hlásná služba	10	3	26,32	7,89
Státní správa a samospráva	26	10	68,42	26,32
Soc. ochrana a zaměstnanost	10	3	26,32	7,89
Justice a vězeňství	16	3	42,11	7,89

Výpočty os

$$O_1 = 100 - \left(\frac{K_{ar\,\max} - K_{ar\,\min}}{100} \right) \cdot s = 100 - \left(\frac{68.42 - 0}{100} \right) \cdot 90 = \underline{\underline{38.42\%}}$$

$$O_2 = 100 - \left(\frac{K_{pr\,\max} - K_{pr\,\min}}{100} \right) \cdot s = 100 - \left(\frac{71.05 - 0}{100} \right) \cdot 90 = \underline{\underline{36.06\%}}$$

Příloha 6 Výsledná graf analýzy souvztažnosti



Příloha 7 Matice rizik

		Energetika				Vodní hospodářství			Potravinářství a zemědělství			Zdravotní péče				Doprava				Komunikační a informační systémy							Bankovní a finanční sektor				Nouzové služby					Veřejná správa			
		Elektřina	Plyn	Tepelná E	Ropa	Zás.pit.vodou	Povrchové vody	Odpadní vody	Produkce potravin	Péče o potraviny	Zemědělská výroba	Přednem. neod.péče	Nemocniční péče	Ochrana veř. zdraví	Léčiva	Silniční	Železniční	Letecká	Vnitrozemská vodní	Služby pevných TS	Služby mobilních TS	Radiová komunikace	Satelitní komunikace	Televize a rádio	Poštovní služby	Internet a data	Správa veřejných fin.	Bankovnictví	Pojišťovnictví	Kapitálový trh	HZS a JPO	PČR	AČR	Radiační mon. síť	Předpovědní, hlásná služba	Státní správa a samospráva	Soc. ochrana	Justice a vězeňství	ΣK_{ar}
Energetika	Elektřina		1	0	1	1	1	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	8
	Plyn	0		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1
	Tepelná E	1	1		0	0	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	5
	Ropa	1	0	0		0	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	6
Vodní hospodářství	Zás. pit. a už. vodou	1	0	0	0		1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3
	Povrchové vody	0	0	0	0	0		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Odpadní vody	1	0	0	0	0	1		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2
Potravinářství a zemědělství	Produkce potr.	1	1	1	1	1	0	0		1	1	0	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	10
	Péče o potr.	1	1	1	1	1	0	0	1		1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	7
	Zem. výroba	0	0	1	1	1	1	1	1	1		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	7
Zdravotní péče	Přednem. neod.péče	0	0	0	1	1	0	0	0	0	0		1	0	1	1	0	0	0	0	0	1	0	0	0	0	1	0	0	0	1	1	0	0	0	1	0	0	10
	Nemocniční p.	1	1	1	0	1	0	1	1	0	0	0		1	1	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	1	0	0	11
	Ochr. veř. zdraví	0	0	0	0	1	1	1	1	0	0	1	1		1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	8
	Léčiva	1	1	1	1	1	0	0	0	0	0	0	0	0		1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	7
Doprava	Silniční	0	0	0	1	0	0	0	0	0	0	0	0	0	0		0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	1	0	0	0	0	0	0	4
	Železniční	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0		0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	4
	Letecká	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0		0	0	0	1	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	6
	Vnitrozemská vodní	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0		0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	4
Komunikační a informační systémy	Služby pevných TS	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		1	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	4
	Služby mobilních TS	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	3
	Rádiová komunikace	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	2
	Satelitní komunikace	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1
	Televize a rádio	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1		0	1	0	0	0	0	0	0	0	0	0	0	0	0	4
	Poštovní služby	1	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	1	0	0		1	0	0	0	0	0	0	0	0	0	0	0	0	6
	Internet a data	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	0	0		0	0	0	0	0	0	0	0	0	0	0	0	4
Bankovní a finanční sektor	Správa veřejných fin.	1	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1		1	1	1	1	1	0	0	0	1	0	0	12
	Bankovnictví	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	1	1	0		1	1	0	0	0	0	0	0	0	0	7
	Pojišťovnictví	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	1	1	0	1		1	0	0	0	0	0	0	0	0	7
	Kapitálový trh	1	1	0	1	0	0	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	1	0	1	0	1	1		0	0	0	0	0	0	0	0	10
Nouzové služby	HZS a JPO	1	0	0	1	1	1	1	0	0	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	1	1	0	0	0		1	1	1	1	1	0	0	14
	PČR	1	0	0	1	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	1	1	0	0	0	1		1	0	0	1	1	1	12
	AČR	0	0	1	1	1	1	0	1	0	0	0	0	0	0	1	0	0	0	0	0	1	1	0	0	1	1	0	0	0	1	1		1	1	1	0	0	15
	Radiační mon. síť	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	1	0	1		1	1	0	0	7
	Předpovědní, hlásná služba	1	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	1	1	0	0	0	1	0	1	1		1	0	0	10
Veřejná správa	Státní správa a samospráva	1	0	1	1	1	0	1	1	0	0	0	1	1	0	1	1	0	0	1	1	0	1	0	1	1	1	1	1	1	1	1	1	1	1		1	1	26
	Soc. ochrana a zaměstnanost	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	1	1	1	0	1	0	0	0	1	1		1	10
	Justice a vězeňství	1	0	1	1	1	0	1	1	0	0	0	0	0	0	1	0	0	0	0	0	1	0	0	1	1	1	0	0	0	1	0	0	0	1	1	1		16
	ΣK_{pr}	27	8	8	20	15	11	7	7	2	2	1	3	2	3	12	6	2	0	6	5	13	6	1	7	26	11	5	5	7	8	8	6	4	3	10	3	3	